Bondarenko N., Sytnichenko O. Organizacijno-pravove zabezpechennja informacijnoi' bezpeky pidpryjemstv. *Zovnishnja torgivlja: ekonomika, finansy, pravo*. 2023. № 2. S. 76-87. Serija. Jurydychni nauky. https://doi.org/10.31617/3.2023(127)05

УДК 346.14:[004.056.5:334.7

DOI: 10.31617/3.2023(127)05

БОНДАРЕНКО Наталія,
к. ю. н., доцент, доцент кафедри правового забезпечення безпеки бізнесу Державного торговельно-економічного університету
вул. Кіото, 19, м. Київ, 02156, Україна
ORCID: 0000-0001-9370-301X
n.bondarenko@knute.edu.ua

BONDARENKO Natalia,
PhD (Law), Associate Professor, Associate Professor of the Department of Legal Security of Business
State University of Trade and Economics
19, Kyoto St., Kyiv, 02156, Ukraine
ORCID: 0000-0001-9370-301X
n.bondarenko@knute.edu.ua

СИТНИЧЕНКО Олена,
к. ю. н., доцент, доцент кафедри правового забезпечення безпеки бізнесу Державного торговельно-економічного університету
вул. Кіото, 19, м. Київ, 02156, Україна
ORCID:0000-0002-9740-0216
o.sytnichenko@knute.edu.ua

SYTNICHENKO Olena,
PhD (Law), Associate Professor, Associate Professor of the Department of Legal Security of Business
State University of Trade and Economics
19, Kyoto St., Kyiv, 02156, Ukraine
ORCID:0000-0002-9740-0216
o.sytnichenko@knute.edu.ua

ОРГАНІЗАЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

Вступ. *У контексті європейської інтеграції від інформаційної безпеки залежить ефективність роботи національних підприємств, а в кінцевому підсумку – ступінь захищеності суспільних інтересів країни, інформаційних прав людей і громадян.*

Проблема. *В умовах воєнної та інформаційної агресії проти України важливим є організаційно-правове забезпечення інформаційної безпеки підприємств, що включає аналіз законодавчої бази в цій сфері, а також дослідження персоналу, який може стати джерелом витоку інформації.*

Метою *статті є оцінка правового регулювання інформаційної безпеки підприємств з погляду їх організаційної складової та визначення загроз витоку інформації, що їх може створювати персонал підприємства у зв'язку з доступом до конфіденційної, таємної та службової інформації.*

Методи. *Використано низку філософських, загальнонаукових, спеціально-наукових принципів і методів: діалектичний, порівняльного аналізу, системний, аналізу та синтезу, формально-юридичний.*

Результати. *Нормативно-правове регулювання інформаційної безпеки в Україні забезпе-*

ORGANIZATIONAL AND LEGAL PROVISION OF INFORMATION SECURITY OF ENTERPRISES

Introduction. *Within the framework of European integration, the effectiveness of the work of national enterprises depends on the information security, and ultimately the degree of protection of the public interests of the country, the informational rights of people and citizens.*

Problem. *In the conditions of military and informational aggression against Ukraine, it is important to ensure organizational and legal information security of enterprises, which includes the analysis of the legislative framework in this area, as well as the study of personnel who may become a source of information leakage.*

The aim *of the article is to assess the legal regulation of information security of enterprises from the point of view of their organizational component and to determine the threats of information leakage that may be created by the enterprise personnel in connection with access to confidential, secret and official information.*

Methods. *A number of philosophical, general scientific, special scientific principles and methods are used: dialectical, comparative analysis, systemic, analysis and synthesis, formal and legal.*

Results. *Normative and legal regulation of information security in Ukraine is ensured by the*

Автори не отримували прямого фінансування для цього дослідження.

Внесок авторів є рівнозначним.

чується Конституцією України, низкою законів та інших нормативно-правових документів.

Для усунення небезпек і загроз діяльності підприємству варто проаналізувати зовнішнє й внутрішнє середовище його діяльності та усунути чинники деструктивного характеру. Важливим у цьому контексті є контроль допуску працівників до роботи з документами й матеріалами, що мають інформацію з обмеженим доступом. Важливим інструментом також є корпоративна етика.

Висновки. *Україні вдалося досягти певних успіхів щодо нормативно-правового регулювання забезпечення інформаційної безпеки, хоча лишилася низка недоліків.*

Забезпечити інформаційну безпеку підприємствам дає змогу використання сучасних кадрових технологій. Працівники, що винні в розголошенні відомостей, які мають комерційну таємницю, згідно з ч. 6 ст. 36 ГК України несуть відповідальність, установлену законом – дисциплінарну, матеріальну, цивільну, адміністративну або кримінальну. Важливим елементом інформаційної безпеки підприємств є контроль, який покладається на його службу безпеки.

Ключові слова: інформаційна безпека підприємства, інформація з обмеженим доступом, служба безпеки підприємства, корпоративна етика.

Constitution of Ukraine, a number of laws and other normative and legal documents.

In order to eliminate dangers and threats to the company's activity, it is necessary to analyse the external and internal environment of its activity and eliminate factors of a destructive nature. In this context, it is important to control the access of employees to work with documents and materials that contain information with limited access. Corporate ethics is also an important tool.

Conclusions. *Ukraine managed to achieve certain successes in terms of normative and legal regulation of information security, although a number of shortcomings remained.*

The use of modern personnel technologies allows enterprises to ensure information security. Employees who are guilty of disclosing information that is a commercial secret, in accordance with Part 6 of Art. 36 of the Civil Code of Ukraine bear responsibility established by law – disciplinary, material, civil, administrative or criminal. An important element of information security of enterprises is control, which is entrusted to its security service.

Keywords: enterprise information security, information with limited access, enterprise security service, corporate ethics.

JEL Classification: M14, J53, K39.

Конфлікт інтересів: Автори заявляють, що вони не мають фінансових чи нефінансових конфліктів інтересів щодо цієї публікації; не мають відносин із державними органами, комерційними або некомерційними організаціями, які могли б бути зацікавлені у поданні цієї точки зору. З огляду на те, що автори працюють в установі, яка є видавцем журналу, що може зумовити потенційний конфлікт або підозру в упередженості, остаточне рішення про публікацію цієї статті (включно з вибором рецензентів та редакторів) приймалося тими членами редколегії, які не пов'язані з цією установою.

Вступ. У контексті європейської інтеграції з метою корекції базових функцій країни мають бути створені умови для розвитку свободи інформації, стратегічні орієнтири впровадження стандартів НАТО, а також ефективна політика державного управління в проєктах інформаційної безпеки (далі – ІБ). На сьогодні варто дослідити організаційно-правові засади ІБ, від яких залежить ефективність роботи національних підприємств, а в кінцевому підсумку – ступінь захищеності суспільних інтересів країни, інформаційних прав людей і громадян.

Проблема. Забезпечення прав, свобод і законних інтересів громадян має пріоритетний напрям діяльності органів публічної влади України. Наразі, усвідомлюючи особливості інформаційної безпеки України, що пов'язано з активною військовою та інформаційною агресією проти нашої країни, виникає потреба дослідити важливий складовий її елемент – організаційно-правове забезпечення ІБ підприємств у нашій державі, що включає аналіз законодавчої бази в цій сфері, а також дослідження персоналу, який може стати джерелом витоку інформації з різними режимами доступу.

Аналіз останніх досліджень і публікацій. Окремі аспекти дослідження цієї проблематики знайшли своє відображення у працях Р. Калюжного та О. Баєва, які дослідили особливості нормативно-правового забезпечення ІБ України [1], Т. Шири, яка виокремила поняття «загрози кадрової безпеки» підприємства [2]. ІБ у підприємницькій діяльності стала об'єктом дослідження юриста-безпекознавця М. Зубка [3]. Проблематика притягнення працівника до юридичної відповідальності за розголошення комерційної таємниці розглянута науковцем Т. Алієвим [4]. О. Галюк зазначила шляхи підвищення корпоративної етики як ефективного інструментарію забезпечення економічної безпеки підприємства [5]. Однак комплексне дослідження запропонованої проблематики наразі залишається відсутнім.

Метою статті є оцінка правового регулювання інформаційної безпеки підприємств з огляду на їх організаційну складову та визначення загроз витоку інформації, що їх може створювати персонал підприємства внаслідок доступу до конфіденційної, таємної та службової інформації.

Методи. Методологічною основою статті є низка філософських, загальнонаукових, спеціально-наукових принципів і методів: діалектичний, порівняльного аналізу, системний, аналізу та синтезу, формально-юридичний.

Результати дослідження. Після проголошення Україною незалежності розпочався новий етап розвитку та становлення національного законодавства, зокрема й у сфері забезпечення інформаційної безпеки. Чинні нормативно-правові акти регулюють особливості взаємовідносин між суб'єктами ІБ, визначаючи їхні права, обов'язки та відповідальність, окреслюють дії суб'єктів ІБ на всіх рівнях, а саме людини, суспільства, держави, а також організаційні засади їхньої діяльності, встановлюють порядок застосування різних сил і засобів забезпечення ІБ.

Нормативно-правове регулювання ІБ в Україні гарантовано Конституцією України [6], Законами України «Про інформацію» [7], «Про національну безпеку України» [8], «Про доступ до публічної інформації» [9], Кодексами України – цивільним, кримінальним, господарським, про адміністративні правопорушення, про працю [10–14]; указами Президента України, якими в 2017 р. затверджено Доктрину інформаційної безпеки України, а в 2021 р. – Стратегію кібербезпеки України [15; 16]; Постановою КМУ «Про перелік відомостей, що не становлять комерційної таємниці» [17].

Аналіз нормативно-правового забезпечення ІБ загалом та її суб'єктів господарювання (підприємств) зокрема свідчить, що нині ця діяльність врегульована достатньою кількістю законів і підзаконних нормативно-правових актів. Проте у правовому регулюванні спостерігаються деякі недоліки, пов'язані з тим, що ці акти приймалися в різні часи без узгодження понятєвого апарату та мають низку не

цілком коректних термінів або взагалі не мають їх чіткого визначення. Наразі в законодавстві відсутня дефініція «*інформаційна безпека*», попри те, що це поняття дуже часто застосовується в практичній діяльності. Так, в профільному Законі України «Про інформацію» законодавець лише обмежився закріпленням базових понять, зокрема «інформація», «захист інформації» [7]. Цілком погоджуємось з Р. Калюжним та О. Баєвим, які зазначають, що досі не вирішеними залишаються питання щодо коректності визначення термінів «таємна інформація», «таємниця», «документована інформація», «автоматизовані системи», «системи інформаційних відносин» [1]. Така ситуація лише створює складнощі у практичній діяльності суб'єктів господарювання у сфері забезпечення інформаційної безпеки.

Через застосування російською федерацією технологій інформаційної війни проти України, а також використовуючи найновіші інформаційні технології впливу на свідомість громадян, що спрямовано на розпалювання національної та релігійної ворожнечі, пропаганди агресивної війни, зміни конституційного ладу насильницьким шляхом або порушення суверенітету й територіальної цілісності України у 2021 р. Указом Президента затверджена нова Стратегія кібербезпеки України, в якій зроблено акцент на кібербезпеці як одному з пріоритетних напрямів системи національної безпеки України. Метою Стратегії є створення умов для безпечного функціонування кіберпростору з подальшим використанням в інтересах особи, суспільства і держави [16].

Наразі в Україні досягнуто певних успіхів щодо нормативно-правового регулювання забезпечення ІБ. Це обумовлено тим, що забезпечення ІБ стало одним з пріоритетних напрямів діяльності органів влади, адже сучасне інформаційне середовище активно впливає на стан політичної, економічної, військової та інших складових як національної безпеки України загалом, так і окремих господарюючих суб'єктів. Аналіз цього нормативно-правового забезпечення свідчить, що сучасна ІБ є самостійною сферою національної безпеки, яка містить організаційно-правове забезпечення ІБ підприємств в Україні, їхніх інформаційних ресурсів, поширення та використання інформаційної інфраструктури, захист таємної та конфіденційної інформації, інформації про особу. Нині правове регулювання щодо забезпечення ІБ підприємств має цілісний характер, проте окремою його складовою є необхідність дослідити персонал підприємства, який може стати джерелом небезпек і загроз його діяльності (наприклад, витік інформації, доступ до таємної, конфіденційної, службової інформації тощо).

Отже, формування ефективних заходів системи інформаційної безпеки підприємства залежить від його кадрового потенціалу та забезпечує стабільне функціонування в умовах ринкової економіки. Згідно з науковими дослідженнями, за участі персоналу компанії

здійснюється 80 % спроб злому мереж і отримання несанкціонованого доступу до комп'ютерної інформації [18, с. 9].

Зазначені явища свідчать, що персонал підприємства стає однією з загроз витоку інформації, що вимагає сформувати поняття *кадрової безпеки підприємства*. На нашу думку, це комплекс дій і взаємовідносин персоналу, завдяки якому відбувається ефективне економічне та інформаційне функціонування підприємства, підвищується здатність протистояти внутрішнім і зовнішнім загрозам та проводиться прогнозування впливу персоналу на показники роботи у трудових правовідносинах. Кадрова безпека на підприємствах здійснюється за такими напрямами: відбір та перевірка кандидатів на вакантні посади; розроблення мотиваційних схем оплати праці робітників і проєктування кар'єри; ліквідація витрат під час трудових спорів; підвищення надійності співробітників; вивчення ситуації у конкурентів; аналіз сайтів вакансій і кадрових агентств, дослідження ринку праці в регіоні; розгляд підприємства з погляду роботодавця.

Для усунення небезпек і загроз діяльності підприємству варто проаналізувати зовнішнє й внутрішнє середовище його діяльності та усунути чинники деструктивного характеру.

Можливість завдання збитків конкретному підприємству є сутністю загрози безпеці його інтересам. За теорією та практикою слід розрізняти поняття «небезпека» і «загроза». Спільним у змісті *загрози* і *небезпеки* є їхня можливість завдати шкоду, а відмінності полягають у характері та ступені готовності суб'єкта до заподіяння збитку. Зокрема на відміну від загрози у *небезпеці* суб'єкт залишається чітко невираженим, а її характер – непевний та безадресний. Крім цього, небезпека – це уявна готовність до завдання шкоди, а загроза – це явні наміри її заподіяти. *Загрози* виникають під дією внутрішніх і зовнішніх чинників, їм завжди притаманна реальна динаміка; вони завдають збитки та порушують порядок роботи підприємства, а відтак вимагають від підприємства вживати комплексні заходи для їхнього усунення та нейтралізації [2, с. 533].

Загроза інформаційній безпеці підприємства на відміну від небезпеки завжди має адресний характер, чітко виражений суб'єкт і об'єкт, встановлену спрямованість – завдання йому шкоди. Суб'єктами загроз інформаційної та кадрової безпеки можуть бути претенденти на вакантну посаду, працюючі та звільнені робітники. Об'єктом загроз виступають зазвичай інформаційні, людські та фінансові ресурси компанії. Розглянемо персонал як об'єкт безпеки: суб'єктом загроз можуть виступати роботодавець, кримінальне оточення, соціальні структури. Тож загрози кадровій безпеці мають двовекторний характер, оскільки персонал компанії може бути одночасно і суб'єктом, і об'єктом загроз. Відповідно, людські ресурси у відносинах кадрової безпеки, з одного боку, потребують свого захисту, а з іншого – можуть виступати як джерело небезпеки та

загрози. Збалансованість інтересів усіх учасників соціально-трудових відносин є запорукою забезпечення безпеки кадрів.

Попередити виникнення загроз ІБ підприємства може вивчення чинників, які їх провокують [3, с. 86]. До *внутрішніх чинників* належать: відсутність корпоративної етики; низька ефективність контролю на етапах відбору персоналу на вакантну посаду та його перевірки у процесі трудових правовідносин; невисокий рівень соціальної відповідальності бізнесу (затримання виплати заробітної плати, неефективна система мотивації персоналу, неграмотна політика щодо звільнення працівників); недостатнє опрацювання нормативно-правової бази в галузі забезпечення кадрової безпеки персоналу; відсутність ефективної політики на підприємстві щодо навчання персоналу основам протидії загрозам кадровій безпеці. До *зовнішніх чинників*, які провокують виникнення інформаційних загроз на підприємстві, відносять: кращі умови мотивації у конкурентів та їхня настанова на переманювання; зовнішній тиск на працівників; їхнє потрапляння у різні види залежності; інфляційні процеси.

Особливості допуску працівників до роботи з документами й матеріалами, які мають інформацію з обмеженим доступом, в Україні врегульовано Цивільним кодексом (ЦК) [10], Господарським кодексом (ГК) [13], Законами України «Про інформацію» [7], «Про доступ до публічної інформації» [9].

Інформацією, за ст. 1 Закону України «Про інформацію», є публічно оголошені або документовані відомості про явища та події, що відбуваються у державі, суспільстві та навколишньому середовищі. Внутрішній спосіб «соціалізації» інформації – це розповсюдження відомостей серед обмеженого кола осіб через спеціалізовані документи, а зовнішній спосіб – оприлюднення інформації невизначеному колу осіб.

За режимом доступу інформація поділяється на відкриту та з обмеженим доступом, що врегульовано ст. 20 Закону України «Про інформацію». До того ж інформація з обмеженим доступом поділяється на конфіденційну, таємну та службову (ст. 6 ЗУ «Про доступ до публічної інформації»).

Конфіденційна інформація, відповідно до ч. 2 ст. 21 ЗУ «Про інформацію» та ст. 7 ЗУ «Про доступ до публічної інформації», – це відомості, які знаходяться у володінні, користуванні та розпорядженні окремих фізичних або юридичних осіб, поширюється за їх бажанням щодо передбачених ними умов.

Таємну інформацію, згідно зі ст. 8 ЗУ «Про доступ до публічної інформації», утворюють державна, професійна, банківська та інші передбачені законом таємниці, розголошення яких може завдати шкоди особі, державі та суспільству. Банківська таємниця є різновидом комерційної й виступає об’єктом інтелектуальної власності згідно зі ст. 420 Цивільного кодексу України (ЦКУ).

Службова інформація, за ст. 9 ЗУ «Про доступ до публічної інформації», характеризує доступ до неї обмеженого кола виконавців зі специфічними службовими обов'язками, яким заборонено розголошувати ці відомості. Така інформація не пов'язана з комерційною цінністю, має гриф «для службового користування», а її перелік встановлюється органами державної влади та місцевого самоврядування.

Дещо інша ситуація з відомостями, що мають *комерційну таємницю*, яка відповідно до ст. 505 ЦК України є інформацією секретною в тому розумінні, що вона загалом чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якої вона належить, через це має комерційну цінність та є предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Особами, що законно контролюють комерційну таємницю, з огляду на аналіз норм цивільного та господарського законодавства, можуть бути як сам власник (ст. 36 ГК), так і наймані працівники, яким надано цю інформацію на підставі трудового договору, контрагенти суб'єкта господарювання на підставі цивільноправової угоди, або працівники судових і правоохоронних органів внаслідок виконання ними своїх службових обов'язків та у випадках, передбачених законодавством. На всіх зазначених суб'єктів розповсюджуються обов'язки щодо вжиття заходів із збереження секретності цієї інформації.

ЦК та ГК України до комерційної таємниці відносять відомості виробничого, технічного, комерційного та організаційного характеру. Конкретний перелік відомостей, що мають комерційну таємницю підприємства, законодавчо не визначений. На думку цивіліста О. Підопригори, це створює проблему практичного характеру, оскільки у такій інформації немає що захищати (охоронних документів на комерційну таємницю ніхто не видає, офіційної її реєстрації не існує). Справою власника залишається захист такої інформації [3, с. 109], який має певні умови.

Самостійне визначення власником підприємства кола та обсягу інформації, яка буде складати для нього комерційну таємницю (ч. 1 ст. 36 ГК). Для цього підприємство повинне розробити та затвердити наказом Положення про комерційну таємницю з переліком відомостей, які її становлять та принципами регулювання й поводження персоналу з такою інформацією. Окремо затверджується Перелік відомостей, що становлять комерційну таємницю, в якому інформація має бути викладена так, щоб працівники мали чітке уявлення, про які самі дані йдеться. Фахівці-безпекознавці рекомендують включити відповідний розділ до Статуту підприємства. Також до трудових

договорів і посадових інструкцій працівників мають бути внесені пункти про нерозголошення комерційної таємниці.

Практика діяльності суб'єктів господарювання показує, що до комерційної таємниці належить: інформація про складання бізнес-плану діяльності підприємства; його прибутковість; цінова політика; договірна діяльність (інформація щодо постачальників та покупців); ноу-хау, яке не захищено авторським і патентним правом; власні аналітичні огляди ринку та маркетингові дослідження.

Власник повинен вжити заходів щодо обмеження доступу третіх осіб до комерційної таємниці на законній підставі. У такому випадку виняток можуть становити тільки ті відомості, які згідно з Постановою КМУ від 09.08.93 р. № 611 не можуть належати до комерційної таємниці [17].

Порушення законодавства про працю у разі розголошення комерційної таємниці буде мати місце лише за умов, якщо працівник дав письмову згоду про нерозголошення комерційної таємниці, а вимоги її нерозголошення закріплені в посадових інструкціях і трудових договорах з працівником, правилах внутрішнього трудового розпорядку та у відповідних внутрішніх документах підприємства, про які ми зазначили.

Для доведення факту розголошення комерційної таємниці конкретним працівником варто зібрати якомога більше доказів його протиправної поведінки, зокрема дані відеозапису, що ведеться у приміщеннях, які мають секретну інформацію; покази свідків, присутніх під час розголошення працівником комерційної таємниці тощо. При цьому роботодавець має дотримуватись конституційного права працівників на таємницю листування, телефонних переговорів та іншої кореспонденції, оскільки згідно зі ст. 31 Конституції України обмеження такого права допускається лише в судовому порядку.

Працівники, винні у розголошенні відомостей, що становлять комерційну таємницю, згідно з ч. 6 ст. 36 ГК України несуть відповідальність, установлену законом – дисциплінарну, матеріальну, цивільну, адміністративну або кримінальну [4]. Так, за порушення працівником зобов'язань щодо нерозголошення комерційної таємниці або іншої захищеної законом інформації роботодавець може притягнути його до дисциплінарної відповідальності – звільнити на підставі ст. 147 КЗпП. Якщо через таке порушення роботодавцеві завдано прямої дійсної майнової шкоди, то згідно зі ст. 130 КЗпП працівник притягається до матеріальної відповідальності. Відшкодування працівником цивільно-правової шкоди, заподіяної внаслідок розголошення комерційної таємниці, здійснюється відповідно до загальних положень цивільного законодавства з урахуванням загального строку позовної давності в три роки (ч. 1 ст. 257 ЦК). Розголошення комерційної таємниці посадовими особами підприємств, приватними підприємцями, працівниками

на користь третіх осіб передбачає адміністративну відповідальність у порядку ч. 3 ст. 164-3 КпАП. За вчинення такого порушення з корисливих чи інших особистих мотивів, якщо це завдало істотної шкоди суб'єкту господарської діяльності, настає кримінальна відповідальність у порядку, передбаченому ст. 232 КК України.

Організаційно-правове забезпечення ІБ підприємства здійснює служба безпеки підприємства, яка захищає його інтереси та ресурси. Спостереження за діями персоналу забезпечуються відкритістю роботи. Фахівці з безпеки рекомендують розташовувати робочі місця у відкритому середовищі, здійснювати облік виконаної роботи, оголошувати результати контрольних заходів за результатами роботи, аналізувати допущені порушення.

Законність дій поведінки персоналу досягається розробкою нормативної документації, яка визначає об'єктивні вимоги до персоналу; порядок, правила та технології проведення операцій; посадові функції, режими безпеки; відповідальність працівників за порушення трудової дисципліни.

Законність має зачіпати не тільки професійні вимоги до працівників, а й морально-етичну і соціальну-економічну сторони взаємовідносин персоналу з адміністрацією (кар'єрне зростання, соціальний пакет, належні умови праці, гідну зарплату). У такому разі для працівника втрачається сенс діяти протиправно, бо він розуміє, що втратить хорошу роботу.

Методами *профілактики правопорушень* з боку персоналу в системі організаційно-правового забезпечення ІБ підприємства можуть бути: здійснення внутрішнього і зовнішнього аудиту діяльності керівних кадрів; періодичний перерозподіл функціональних повноважень працівників структурного підрозділу; доручення комерційних справ фахівцям на конкурентній основі; додержання сучасних технологій охорони інформаційних ресурсів підприємства; обмеження доступу працівників до документів бухгалтерської звітності; оптимізація системи фінансової звітності [3, с. 126].

Потужним імпульсом виховання надійності працівників стає пропаганда корпоративності шляхом вивчення історії розвитку підприємства, порівняння результатів його діяльності з конкурентами, проведення тімбілдінгів. *Корпоративна етика* сьогодні стає важливим інструментом ефективного управління персоналом підприємства й забезпечує його інформаційну безпеку [5, с. 180].

Побудова ефективної корпоративної етики в організації є складним завданням, оскільки визначити єдиний стандарт поведінки людей неможливо. На неї впливатимуть різні чинники – національність, релігія, світогляд людини, її виховання та інше. Однак у межах організації можливо окреслити певні норми та правила поведінки персоналу та розробити механізми мотивування й відповідальності за її дотримання.

Висновки. Україні вдалося досягти певних успіхів у нормативно-правовому регулюванні забезпечення інформаційної безпеки. Це насамперед обумовлено тим, що забезпечення ІБ стало одним з пріоритетних напрямів діяльності органів державної влади, адже сучасне інформаційне середовище активно впливає на стан політичної, економічної, військової та інших складових як національної безпеки загалом, так і окремих господарюючих суб'єктів. Аналіз організаційно-правового забезпечення ІБ підприємств свідчить, що нині така діяльність регулюється як законами, так і підзаконними нормативно-правовими актами. Проте у правовому регулюванні є й недоліки – ці акти приймалися в різний час без узгодження понятійного апарату, мають низку некоректних термінів або взагалі не мають чіткого їх визначення.

Забезпечити ІБ підприємствам дає змогу використання сучасних кадрових технологій, зокрема: атестація працівників, запобігання конфліктним ситуаціям, прискорена адаптація через наставництво, пропаганда корпоративності, ефективна мотивація.

Працівники, винні у розголошенні відомостей, що мають комерційну таємницю, згідно з ч. 6 ст. 36 ГК України несуть відповідальність, установлену законом – дисциплінарну, матеріальну, цивільну, адміністративну або кримінальну.

Важливим елементом ІБ підприємств є контроль, який покладається зазвичай на службу безпеки підприємства і комплекс засобів (обмежувальні режими, оцінювальні операції, технологічні процеси, регламенти), що встановлено для працівників і адміністрації з метою ліквідувати можливості заподіяти збитки підприємству внаслідок витоку інформації. Корпоративна етика сьогодні також стає важливим інструментом, що забезпечує його інформаційну безпеку підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Калюжний Р., Баєв О. Нормативно-правове забезпечення інформаційної безпеки України. *Правова інформатика*. 2009. № 4(24). С. 5-12.
2. Шира Т. Загрози кадрової безпеки підприємства. *Економіка і суспільство*. 2016. №7. С. 532-535.
3. Зубок М. Інформаційна безпека в підприємницькій діяльності. Київ. ГНОЗІС, 2015. 2016 с.
4. Алієв Т. Як покарати працівника за розголошення комерційної таємниці. *Зарплата і кадри*. 23.05.2019. URL: https://uteka.ua/ua/publication/commerce-12-zarplaty-i-kadry-3-kak-nakazat-rabotnika-za-razglasheniekommercheskoj-tajny
5. Галюк О. Шляхи підвищення культури підприємництва або «корпоративна етика» як засіб виховання бізнесмена. *Галицький економічний вісник.* 2020. №63 (2). С.176-182.
6. Конституція України: Закон від 28.06.1996 № 254к/96. ВР. База даних «Законодавство України» / ВР України. URL: http//zacon2.rada.gov.ua/laws/show (дата звернення: 09.03.21).
7. Закон України про інформацію. *Відомості Верховної Ради України (ВВР).* 1992. №48. Ст. 650. База даних «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 11.03.21).

8. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. *Відомості Верховної Ради України*, 2018. № 31. С. 241.
9. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. *Голос України*. 2011. № 24. С. 7.
10. Цивільний кодекс України. Закон України від 16 січня 2003 р. № 435-IV. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/435-15#
11. Кримінальний кодекс України від 5 квіт. 2001 р. *Відомості Верховної Ради України*. 2001. № 25-26. С. 131.
12. Кодекс України про адміністративні правопорушення від 7 груд. 1984 р. *Відомості Верховної Ради Української РСР*. 1984. Додат. до № 51. С. 1122.
13. Господарський кодекс України. *Відомості Верховної Ради України (ВВР).* 2003. №18. №19-20. №21-22. Ст.144. База даних «Законодавство України». *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/436-15#Text (дата звернення: 10.03.21).
14. Кодекс законів про працю України від 10.12.1971 № 322-VIII. URL: http://www.rada.gov.ua/laws/show/322-08
15. Доктрина інформаційної безпеки України: затверджено Указом Президента України від 25 лютого 2017 року № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374
16. Стратегія кібербезпеки України: затверджено Указом Президента України від 14 травня 2021 №447/2021. Офіційний сайт Президента України. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text
17. Про перелік відомостей, що не становлять комерційної таємниці: Постанова КМУ від 09.08.93 р. № 611. URL: https://zakon.rada.gov.ua/laws/show/611-93-%D0%BF#Text
18. Гапак О. Захист інформації в комп'ютерних системах. Ужгород. 2021. 184 с.

REFERENCES

1. Kaljuzhnyj, R., & Bajev, O. (2009). Normatyvno-pravove zabezpechennja informacijnoi' bezpeky Ukrai'ny [Regulatory and legal provision of information security of Ukraine]. *Pravova informatyka – Legal informatics*, *4(24),* 5-12 [in Ukrainian].
2. Shyra, T. (2016). Zagrozy kadrovoi' bezpeky pidpryjemstva Zagrozy kadrovoi' bezpeky pidpryjemstva [Threats to personnel security of the enterprise]. *Ekonomika i suspil'stvo – Economy and society, 7*, 532-535 [in Ukrainian].
3. Zubok, M. (2015). *Informacijna bezpeka v pidpryjemnyc'kij dijal'nosti* [*Information security in business activities*]. Kyi'v. GNOZIS [in Ukrainian].
4. Alijev, T. (2019). Jak pokaraty pracivnyka za rozgoloshennja komercijnoi' tajemnyci [How to punish an employee for disclosing a commercial secret]. *Zarplata i kadry – Salary and personnel*. https://uteka.ua/ua/publication/commerce-12-zarplaty-i-kadry-3-kak-nakazat-rabotnika-za-razglasheniekommercheskoj-tajny [in Ukrainian].
5. Galjuk, O. (2020). Shljahy pidvyshhennja kul'tury pidpryjemnyctva abo «korporatyvna etyka» jak zasib vyhovannja biznesmena [Ways of improving the culture of entrepreneurship or «corporate ethics» as a means of educating a businessman]. *Galyc'kyj ekonomichnyj visnyk – Galician Economic Bulletin, 63 (2),* 176-182 [in Ukrainian].
6. Konstytucija Ukrai'ny: Zakon vid 28.06.1996 № 254k/96. VR. Baza danyh «Zakonodavstvo Ukrai'ny». VR Ukrai'ny. [Constitution of Ukraine: Law of 28.06.1996 № 254k/96. VR. Database «Legislation of Ukraine». Verkhovna Rada of Ukraine]. http//zacon2.rada.gov.ua/laws/show (data zvernennja: 09.03.21) [in Ukrainian].
7. Zakon Ukrai'ny pro informaciju. *Vidomosti Verhovnoi' Rady Ukrai'ny (VVR)*. 1992. №48. St. 650. Baza danyh «Zakonodavstvo Ukrai'ny». VR Ukrai'ny [Law of Ukraine on information. Information of the Verkhovna Rada of Ukraine (IVR). 1992. №48.

Art. 650. Database «Legislation of Ukraine». Verkhovna Rada of Ukraine]. http://zakon.rada.gov.ua/laws/show/2657-12#Text (data zvernennja: 11.03.21) [in Ukrainian].
8. Pro nacional'nu bezpeku Ukrai'ny: Zakon Ukrai'ny vid 21.06.2018 r. № 2469-VIII [On the national security of Ukraine: Law of Ukraine dated June 21, 2018 № 2469-VIII]. (2018). *Vidomosti Verhovnoi' Rady Ukrai'ny – Information of the Verkhovna Rada of Ukraine*, *31* [in Ukrainian].
9. Pro dostup do publichnoi' informacii': Zakon Ukrai'ny vid 13.01.2011 r. № 2939-VI [On access to public information: Law of Ukraine dated January 13, 2011 № 2939-VI] (2011). *Golos Ukrai'ny – Voice of Ukraine*, *24.* [in Ukrainian].
10. Cyvil'nyj kodeks Ukrai'ny. Zakon Ukrai'ny vid 16 sichnja 2003 r. № 435-IV. Verhovna Rada Ukrai'ny [The Civil Code of Ukraine. Law of Ukraine dated January 16, 2003 № 435-IV. Verkhovna Rada of Ukraine] https://zakon.rada.gov.ua/laws/show/435-15# [in Ukrainian].
11. Kryminal'nyj kodeks Ukrai'ny vid 5 kvit. 2001 r. [The Criminal Code of Ukraine dated April 5 2001] (2001). *Vidomosti Verhovnoi' Rady Ukrai'ny – Information of the Verkhovna Rada of Ukraine, 25-26* [in Ukrainian].
12. Kodeks Ukrai'ny pro administratyvni pravoporushennja vid 7 grud. 1984 r. [Code of Ukraine on Administrative Offenses from December 7 1984] (1984). *Vidomosti Verhovnoi' Rady Ukrai'ns'koi' RSR – Information of the Verkhovna Rada of the Ukrainian SSR*, Додаток до № *51* [in Ukrainian].
13. Gospodars'kyj kodeks Ukrai'ny. *Vidomosti Verhovnoi' Rady Ukrai'ny (VVR)*. 2003. №18. №19-20. №21-22. St.144. *Baza danyh «Zakonodavstvo Ukrai'ny» [Economic Code of Ukraine]. (2003). Vidomosti Verhovnoi' Rady Ukrai'ny (VVR)* St.144. Baza danyh «Zakonodavstvo Ukrai'ny». Vidomosti Verhovnoi' Rady Ukrai'ny – *Information of the Verkhovna Rada of Ukraine*, *18-22.* https://zakon.rada.gov.ua/laws/show/436-15#Text (data zvernennja: 10.03.21) [in Ukrainian].
14. Kodeks zakoniv pro pracju Ukrai'ny vid 10.12.1971 № 322-VIII [Code of Labor Laws of Ukraine dated 10.12.1971 № 322-VIII]. http://www.rada.gov.ua/laws/show/322-08 [in Ukrainian].
15. Doktryna informacijnoi' bezpeky Ukrai'ny: zatverdzheno Ukazom Prezydenta Ukrai'ny vid 25 ljutogo 2017 roku № 47/2017 [Information security doctrine of Ukraine: approved by the Decree of the President of Ukraine dated February 25, 2017 № 47/2017]. https://www.president.gov.ua/documents/472017-21374 [in Ukrainian].
16. Strategija kiberbezpeky Ukrai'ny: zatverdzheno Ukazom Prezydenta Ukrai'ny vid 14 travnja 2021 №447/2021. Oficijnyj sajt Prezydenta Ukrai'ny [Cybersecurity Strategy of Ukraine: approved by the Decree of the President of Ukraine dated May 14, 2021 №447/2021. Official website of the President of Ukraine]. https://zakon.rada.gov.ua/laws/show/447/2021#Text [in Ukrainian].
17. Pro perelik vidomostej, shho ne stanovljat' komercijnoi' tajemnyci: Postanova KMU vid 09.08.93 r. № 611 [About the list of information that does not constitute a commercial secret: Resolution of the CMU of August 9, 1993. № 611]. https://zakon.rada.gov.ua/laws/show/611-93-%D0%BF#Text [in Ukrainian].
18. Gapak, O. (2021). *Zahyst informacii' v komp'juternyh systemah.* [*Protection of information in computer systems.*] Uzhgorod [in Ukrainian].

Надійшла до редакції 28.02.2023.
Прийнято до друку 13.03.2023.
Публікація онлайн 21.04.2023.