УДК 330.837:330.341.1 https://doi.org/10.31713/ve2202213
JEL: M21, O10, P40

Лось З. В. [1; ORCID ID: 0000-0002-1989-5583],
д.е.н., доцент

[1]Національний університет водного господарства та природокористування, м. Рівне

ІННОВАЦІЙНО-КОНЦЕПТУАЛЬНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДІЯЛЬНОСТІ КОРПОРАЦІЙ

У статті досліджено науково-методичні підходи до управління інформаційною безпекою діяльності корпорацій. Розроблено для підвищення інформаційної безпеки діяльності корпорацій концепцію її управління. Розроблено концепцію системної трансформації діяльності корпорацій **в інституційному середовищі. В основі запропонованої концепції покладено розуміння діяльності підприємств як комплексу системних дій, спрямованих на реалізацію єдиного інституційного поля, але не виключає існування і визнання ряду принципів і керівних норм, необхідних для правильного регулювання діяльності таких складних економічних одиниць, що у підсумку призводить до активізації їх діяльності.**

Ключові слова: корпорація; інформатизація; інновація; інформаційна безпека; забезпечення.

Постановка проблеми. На сьогодні захист інформації корпорації є ключовим фактором успіху, корпоративне управління розглядає інформаційну безпеку як бізнес-ризик № 1, яким для ефективного управління потрібно керувати. Якщо розглядати сучасну корпорацію, то варто враховувати, що одним із ризиків кіберзлочинів є ризик управління, для запобігання цього ризику необхідно розширити заходи щодо сприяння інформаційній безпеці всередині корпорації. Розроблення інноваційно-концептуального забезпечення інформаційної безпеки в діяльності корпорацій сприятиме підвищенню інформаційної безпеки діяльності корпорацій.

Аналіз останніх досліджень та публікацій. Сучасні дослідження щодо економічного зростання на основі інноваційної діяльності завдячують інноваційному розвитку, відмітимо, що цій проблематиці присвячені роботи як вітчизняних, так і зарубіжних науковців.

Значний внесок у дослідження теоретичних і прикладних аспектів зробили українські науковці Федулова Л. [1; 2], Сазонець І. [3], Гринько Т. [4], Амоша О., Бажал Ю., Геєць В. та ін. У їх публікаціях

розкрито сутність феномену інноваційного розвитку, розроблені теоретичні принципи й науково-практичні підходи щодо економічного трактування процесу інноваційного розвитку.

У даній роботі Сазонець І. (2021) [3] стверджує, що наука стає реальною рушійною силою розвитку економіки та країни в цілому. Відбувається зміна підходів до провідної суспільної ролі теоретичного знання як джерела нововведень розвитку в постіндустріальному суспільстві.

Разом з тим дискусійними і не до кінця вивченими, залишаються питання теоретичного і прикладного характеру побудови моделі інноваційно-концептуальне забезпечення інформаційної безпеки в діяльності корпорацій.

Мета і завдання дослідження. Метою дослідження є розроблення інноваційно-концептуального забезпечення інформаційної безпеки в діяльності корпорацій в інноваційно-інформаційному середовищі.

Виклад основного матеріалу. Поширення тенденцій інтегрованості національних економік у світове господарство впродовж двох останніх століть відбувається насамперед через розвиток корпоративних відносин. Тим самим стрімкий розвиток корпоративної форми сприяє перетворенню корпоративних структур на домінуючий чинник розвитку світової економіки. Світові тенденції підтверджують, що таким структурам належить провідна роль не лише в інноваційному розвитку, а й в економічному зростанні загалом. Саме завдяки можливостям корпорацій акумулювати значні матеріальні, людські та фінансові ресурси для вирішення науково-технічних і виробничо-господарських завдань відбувається стрімкий розвиток інноваційних технологій і масштабне поєднання з ними виробничих потужностей індустріального суспільства у XX ст. Корпоративні форми підвищують рівень макроекономічного регулювання виробництва, стабільність економічного співробітництва (в тому числі й міжнародного), виступають партнерами держави при розробці та реалізації стратегічної лінії в процесі модернізації економіки. Таким чином, тенденції їхнього «функціонування визначають закономірності розвитку світового господарства і носять універсальний характер. Зокрема, до таких закономірностей слід віднести концентрацію капіталу, інтеграцію промислового і фінансового капіталу, диверсифікацію форм і напрямів діяльності, глобалізацію та інтернаціоналізацію» [2, С. 7].

Динамічний розвиток економічних, політичних, соціальних подій XXI століття сформулював нове уявлення про інформацію як

однин із факторів (ресурсів) виробництва. На макрорівні інформація впевнено займає позиції головного фактора могутності держави, адже здатність держави мати у своєму розпорядженні найсучасніші інформаційні технології дозволяє ефективно управляти інформацією. Володіння державою такою здатністю – шлях до подальшого нарощування своєї економічної міцності [5, С. 2].

На мікрорівні обсяг, достовірність, цілісність, якість обробки інформації визначає ефективність дій менеджменту підприємства, а отже, актуалізує використання інформаційних технологій в управлінні грошово-кредитними, фінансовими, соціально-економічними процесами даного підприємства. «Без необхідного обсягу та якості інформації неможливо забезпечити розвиток суб'єкта господарювання на основі високотехнологічного виробництва, ефективних методів організації праці» [6, С. 34].

Під час дослідження в контексті розгляду наукових підходів до дефініції «інформаційна безпека» було систематизовано та представлено порівняльний аналіз категорії (таблиця).

Таблиця

Підходи до визначення дефініції «інформаційна безпека»

Визначення	Джерело
1	2
Суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності	6, С. 33
Стан інформації, у якому забезпечується збереження визначених політикою безпеки властивостей інформації	7, С. 23
Стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави	8, С. 54
Стан захищеності потреб в інформації особистості, суспільства і держави, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз	9, С. 45
Одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства	10, С. 48

продовження таблиці

1	2
Захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства та держави	11, С. 92
Суспільні правовідносини щодо процесу організації, створення, підтримки, охорони та захисту необхідних для особи (людини чи юридичної особи, установи, підприємства, організації), суспільства і держави безпечних умов їх життєдіяльності; суспільні правовідносини, пов'язані з організацією технологій створення, розповсюдження, зберігання та використання інформації (відомостей, даних, знань) для забезпечення функціонування і розвитку інформаційних ресурсів людини, суспільства, держави	12, С. 3
Стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації	13, ст. 13

Джерело: систематизовано автором на основі [6; 7; 8; 9; 10; 11; 12; 13]

Відповідно до вищезазначеного інформаційну безпеку розглядають за трьома основними характеристиками:

- стан захищеності інформаційного середовища;
- суспільні відносини;
- захищеність встановлених законом правил.

Узагальнюючи підходи до розуміння сутності інформаційної безпеки, слід відмітити, що в умовах інституційної трансформації інформаційну безпеку корпорацій пропонується визначити як інтегровану складову процесу забезпечення захисту інформації від внутрішніх і зовнішніх загроз та створення сприятливих умов для ефективного функціонування корпорацій та підвищення їх конкурентоспроможності.

В якості інноваційно-концептуального механізму забезпечення інформаційної безпеки діяльності корпорацій нами рекомендується комплексний механізм, котрий включає інноваційне забезпечення діяльності корпорацій та забезпечення інформаційної безпеки

діяльності корпорацій для досягнення інноваційного рівня розвитку корпорації та стратегії її розвитку. Авторську структуру інноваційно-концептуального механізму забезпечення інформаційної безпеки діяльності корпорацій представлено на рисунку.

Інноваційне забезпечення діяльності корпорацій передбачає дослідження політико-правого середовища. На даному етапі необхідно провести аналіз та врахування політичної стабільності країни, законодавчо-правове регулювання, а також податкове та антикорупційне регулювання. Зазначимо, що для здійснення ефективної діяльності корпораціям та залучення ПІІ слід змінити законодавчо-правові акти України та адаптувати їх до міжнародних норм, потребує негайного вирішення стабілізація політичного становища всередині держави. Для безперебійної та інноваційної роботи корпорацій необхідно враховувати сприятливе економічне середовище, зокрема, рівень інфляції, ринкове середовище, стадію економічного циклу економіки, власні, позичкові та залучені кошти корпорації.

Своєю чергою забезпечення соціального середовища враховує ставлення до діяльності підприємства, кваліфікацію населення, сприйняття інновацій населенням країни, чисельність населення, комунікації із споживачами, зворотній зв'язок та соціально-економічне забезпечення країни. Забезпечення екологічного середовища включає в себе комплекс заходів, орієнтованих на зменшення рівня забруднення довкілля, клімат, а також географію країни.

Забезпечення технологічного середовища відповідно враховує рівень розвитку науково-технологічного прогресу, рівень інноваційного розвитку країни та маркетингову інформацію тощо.

Забезпечення інституційного середовища – адміністративні санкції, правове регламентування, система стандартів якості.

Забезпечення організаційного середовища – формування організаційних структур управління, ресурсне забезпечення, контроль за зміною пріоритетів, структуру ринка, виробничо-збутова інформація.

Виділимо дев'ять, на нашу думку, основних складових для забезпечення інформаційної безпеки діяльності корпорацій, а саме:

1. Забезпечення відповідальності за безпеку даних передбачає, що корпорація повинна забезпечити, щоб її IT-персонал, робоча сила та керівництво знали про свої обов'язки та що від них очікують. Різні типи даних повинні бути класифіковані таким чином, щоб як працівники, так і менеджери розуміли різницю між ними.

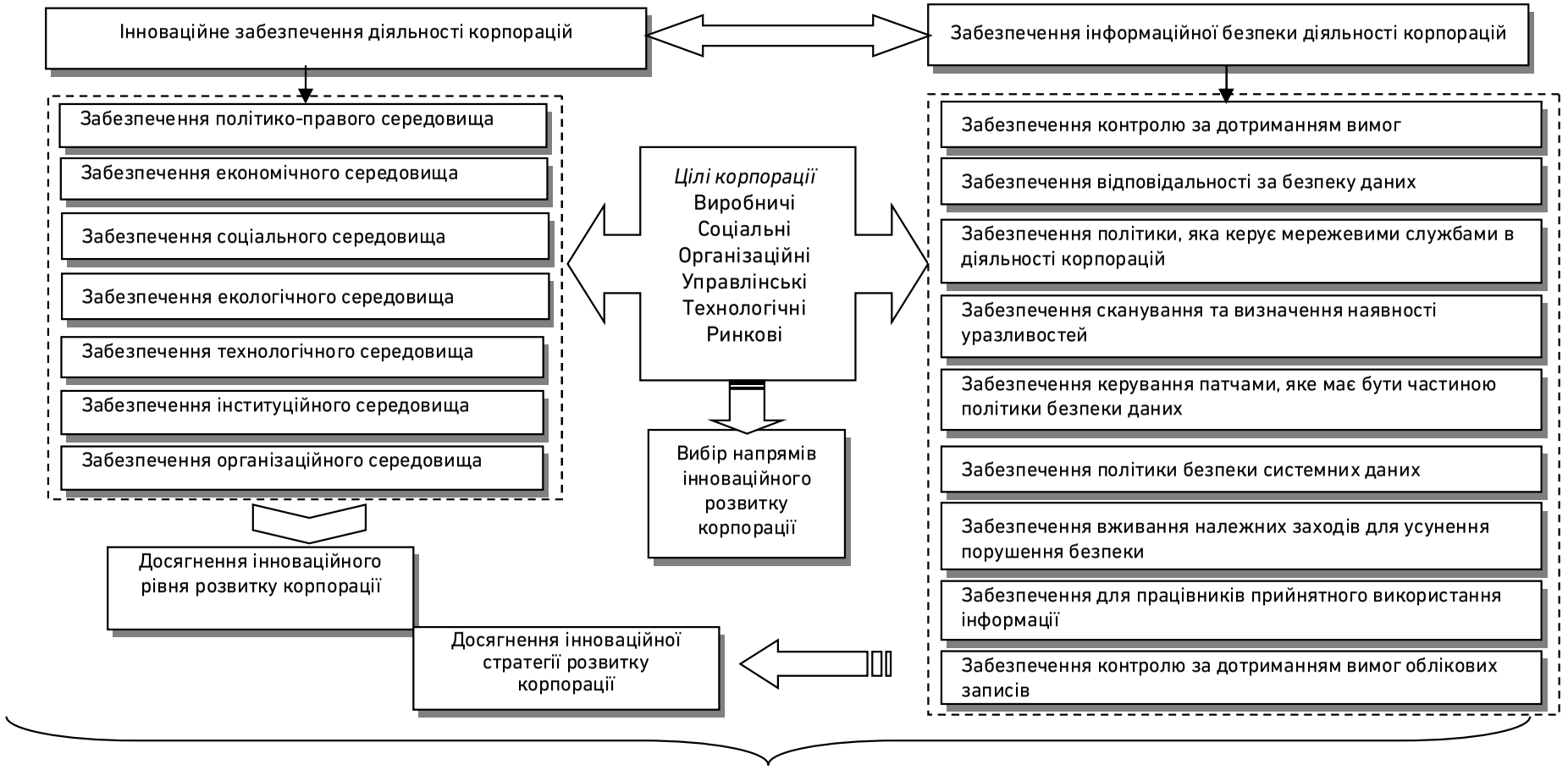

Рисунок. Інноваційно-концептуальний механізм забезпечення інформаційної безпеки діяльності корпорацій
Джерело: авторська розробка

Розподіляючи дані, працівники знають, як обробляти кожен тип і які типи їх дозволено розповсюджувати. Важливими класами для включення в політику є: конфіденційні дані, дані, які призначені для внутрішнього використання в межах корпорації, загальні дані та дані, які можуть бути відправлені за межі компанії.

2. Забезпечення політики, яка керує мережевими службами в діяльності корпорацій. Складова політики безпеки даних визначає, яким чином корпорація повинна займатися такими проблемами, як віддалений доступ, керування та конфігурація IP-адрес. Вона також охоплює безпеку компонентів, таких як маршрутизатори та комутатори. Відмітимо, що саме ця складова має визначати політику щодо виявлення та вторгнення в мережу компанії.

3. Перед хакерами стоїть важливе завдання знайти будь-які чутливі місця для ураження в IT-інфраструктурі корпорації, тому вважаємо, що забезпечення сканування та визначення наявності вразливостей є важливою складовою для забезпечення інформаційної безпеки в діяльності корпорацій. Тому компанія повинна здійснювати рутинну роботу для регулярної перевірки власних мереж.

4. Відмітимо, що частиною політики безпеки даних має бути забезпечення керування патчами. Керування патчами може допомогти захистити від зовнішніх загроз. Як і коли патчі повинні бути введені в систему, це повинно бути частиною політики безпеки даних.

5. На наш погляд, політика безпеки системних даних є критичною частиною політики безпеки даних, оскільки передбачає конфігурацію безпеки усіх важливих серверів та операційних систем. Правила, які стосуються серверів, що працюють в мережах корпорації, а також управління обліковими записами та паролями повинні бути чітко визначені, брандмауер, база даних та антивірусна політика також включені до цієї складової.

6. Зокрема, якщо виникає порушення безпеки, важливо вживати належних заходів для її усунення, саме тому забезпечення належної відповіді на інциденти з порушення безпеки є невід'ємною складовою інноваційно-концептуального забезпечення. Дана складова включає в себе оцінку та звітність про інцидент, а також рішення як усунути проблему, що призвела до цього.

7. Забезпечення для працівників прийнятного використання інформації передбачає чітке визначення того, яка інформація є прийнятною для використання. Окрім того, рекомендується підписати прийнятну політику використання, щоб корпорація могла при необхідності здійснювати дисциплінарні дії.

8. Контроль за дотриманням вимог. Використання аудитів є гарним способом забезпечення того, щоб співробітники та керівництво компанії дотримувалися різних елементів політики щодо захисту даних, відмітимо, що такі перевірки повинні проводитися за регулярним розкладом.

9. Контроль за дотриманням вимог облікових записів або відстеження того, хто має доступ до важливої інформації, є складовою політики захисту даних. Дана складова визначає деякі з найбільш поширених джерел цифрових компромісів, що є законними, але неактивними обліковими записами користувачів. Таке ситуація трапляється, коли співробітник корпорації був звільнений, але його рахунок не було зупинено. Якщо працівник невдоволений, можливість доступу до активів організації може бути надзвичайно шкідливим. Забезпечення інформаційної безпеки в діяльності повинно передбачати призначення конкретних членів IT-групи для ретельного відстеження та контролювання облікових записів користувачів, що дозволить запобігти незаконній діяльності.

Після того, як інноваційна політика забезпечення інформаційної безпеки діяльності корпорацій буде впроваджена корпорацією, вона повинна переглядатися принаймні двічі на рік, щоб бути актуальною. Огляд слід запускати, коли значно вдосконалюються мережеві інфраструктури компанії. Корпорації, котрі серйозно ставляться до запобігання кіберзлочинності та стимулювання, повинні враховувати важливий зв'язок між безпекою даних, конфіденційністю даних та створенням спеціальної політики, яка захищатиме дані, що використовуються корпорацією, тоді дані клієнтів будуть в безпеці.

Розроблений в роботі механізм формування інноваційно-концептуального забезпечення інформаційної безпеки діяльності корпорацій орієнтований насамперед на запобігання кіберзлочинності та стимулювання інноваційного розвитку корпорації.

Реалізація механізму формування інноваційно-концептуального забезпечення інформаційної безпеки діяльності корпорацій дозволить забезпечити такий рівень розвитку, який дозволить повною мірою забезпечити досягнення інноваційної стратегії розвитку корпорації та при цьому отримати найбільшу ефективність з досягненням довгострокових конкурентних переваг.

Висновки. За результатами проведеного дослідження автором розроблено механізм формування інноваційно-концептуального забезпечення інформаційної безпеки діяльності корпорацій, котрий

орієнтований насамперед на запобігання кіберзлочинності та стимулювання інноваційного розвитку корпорації.

Реалізація механізму формування інноваційно-концептуального забезпечення інформаційної безпеки діяльності корпорацій забезпечить такий рівень розвитку, який дозволить в повною мірою забезпечити досягнення інноваційної стратегії розвитку корпорації та при цьому отримати найбільшу ефективність з досягненням довгострокових конкурентних переваг.

1. Федулова Л. І. Концептуальні засади управління інноваційним розвитком підприємств. *Маркетинг і менеджмент інновацій*. 2014. № 2. С. 122–135. **2.** Корпоративні структури в національній інноваційній системі України : монографія / Федулова Л. І., Осецький Л. В., Гончаров Ю. В., Рудченко О. Ю., Бажал Ю. М. К., 2007. 812 с. **3.** Сазонець І. Л., Саленко А. С. Знання та інновації як визначальні детермінанти формування та розвитку постіндустріального суспільства. *Інвестиції: практика та досвід*. 2021. № 11. С. 5–10. **4.** Гринько Т., Шибецька М. Методичні підходи до вибору стратегічних альтернатив розвитку суб'єктів підприємництва. *Управління розвитком*. 2017. № 1–2(187–188). С. 94–100. **5.** Гуцалюк М. Інформаційна безпека України: нові загрози. *Бизнес и безопасность*. 2003. № 5. С. 2–3. **6.** Сороківська О. А., Гевко В. Л. Інформаційна безпека підприємства: нові загрози та перспективи. *Вісник Хмельницького національного університету*. *Економічні науки*. 2010. № 2. Т. 2. С. 32–35. **7.** Хоффман Л. Дж. Современные методы защиты информации. М. : Советское радио, 1980. 57 с. **8.** Богуш В., Юдін О. Інформаційна безпека держави. К. : МК-Прес, 2005. 432 с. **9.** Гуменюк В. Я., Ярошевич Н. Б. Переваги та недоліки застосування функції Кобба-Дугласа як інструменту управління виробничими ресурсами транспортних підприємств. *Вісник Національного університету «Львівська політехніка». Проблеми економіки та управління.* 2000. № 391. С. 157–162. **10.** Литвиненко О. Інформація і безпека. *Нова політика*. 1998. № 1. С. 47–49. **11.** Валіулліна З. В. Управління інформаційною безпекою корпорацій в глобальних інформаційних системах. *Economic development strategy in terms of European integration :* international scientific conference (Kaunas 27 may 2016 year). Kaunas, 2016. С. 103–106. **12.** Кормич Б. А. Інформаційна безпека: організаційно-правові основи : навч. посіб. К. : Кондор, 2008. 384 с. **13.** Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України. URL: https://zakon.rada.gov.ua/laws/show/537-16/stru2 (дата звернення: 10.05.2022).

REFERENCES:

1. Fedulova L. I. Kontseptualni zasady upravlinnia innovatsiinym rozvytkom pidpryiemstv. *Marketynh i menedzhment innovatsii*. 2014. № 2. S. 122–135. **2.** Korporatyvni struktury v natsionalnii innovatsiinii systemi Ukrainy : monohrafiia / Fedulova L. I., Osetskyi L. V., Honcharov Yu. V., Rudchenko O. Yu., Bazhal Yu. M. K., 2007. 812 s. **3.** Sazonets I. L., Salenko A. S. Znannia ta innovatsii yak vyznachalni determinanty formuvannia ta rozvytku postindustrialnoho suspilstva. *Investytsii: praktyka ta dosvid*. 2021. № 11. S. 5–10. **4.** Hrynko T., Shybetska M. Metodychni pidkhody do vyboru stratehichnykh alternatyv rozvytku sub'iektiv pidpryiemnytstva. *Upravlinnia rozvytkom*. 2017. № 1–2(187–188). S. 94–100. **5.** Hutsaliuk M. Informatsiina

bezpeka Ukrainy: novi zahrozy. *Byznes y bezopasnost.* 2003. № 5. S. 2–3. **6.** Sorokivska O. A., Hevko V. L. Informatsiina bezpeka pidpryiemstva: novi zahrozy ta perspektyvy. *Visnyk Khmelnytskoho natsionalnoho universytetu. Ekonomichni nauky.* 2010. № 2. T. 2. S. 32–35. **7.** Hoffman L. Dj. Sovremennyie metodyi zaschityi informatsii. M. : Sovetskoe radio, 1980. 57 s. **8.** Bohush V., Yudin O. Informatsiina bezpeka derzhavy. K. : MK-Pres, 2005. 432 s. **9.** Humeniuk V. Ya., Yaroshevych N. B. Perevahy ta nedoliky zastosuvannia funktsii Kobba-Duhlasa yak instrumentu upravlinnia vyrobnychymy resursamy transportnykh pidpryiemstv. *Visnyk Natsionalnoho universytetu «Lvivska politekhnika». Problemy ekonomiky ta upravlinnia.* 2000. № 391. S. 157–162. **10.** Lytvynenko O. Informatsiia i bezpeka. *Nova polityka*. 1998. № 1. S. 47–49. **11.** Valiullina Z. V. Upravlinnia informatsiinoiu bezpekoiu korporatsii v hlobalnykh informatsiinykh systemakh. *Economic development strategy in terms of European integration :* international scientific conference (Kaunas 27 may 2016 year). Kaunas, 2016. S. 103–106. **12.** Kormych B. A. Informatsiina bezpeka: orhanizatsiino-pravovi osnovy: navch. posib. K. : Kondor, 2008. 384 s. **13.** Pro osnovni zasady rozvytku informatsiinoho suspilstva v Ukraini na 2007–2015 roky : Zakon Ukrainy. URL: https://zakon.rada.gov.ua/laws/show/537-16/stru2 (data zvernennia: 10.05.2022).

Los Z. V. [1; ORCID ID: 0000-0002-1989-5583],
Doctor of Economics, Associate Professor

[1]*National University of Water and Environmental Engineering, Rivne*

INNOVATIVE AND CONCEPTUAL PROVISION OF INFORMATION SECURITY IN THE ACTIVITIES OF CORPORATIONS

The article examines scientific and methodical approaches to information security management of corporations. The purpose of the research is to develop an innovative and conceptual provision of information security in the activities of corporations in an innovative and informational environment. Summarizing the approaches to understanding the essence of information security, it should be noted that in the conditions of institutional transformation, information security of corporations is proposed to be defined as an integrated component of the process of ensuring the protection of information from internal and external threats and creating favorable conditions for the effective functioning of corporations and increasing their competitiveness.

The concept of its management was developed to increase the information security of corporations. The concept of systemic transformation of business entities in the institutional environment has been developed. The basis of the proposed concept is the understanding of the activities of enterprises as a complex of systemic actions aimed at the implementation of a single institutional field, but does not exclude the existence and recognition of a number of principles and guidelines

necessary for the correct regulation of the activities of such complex economic units, which ultimately leads to the activation of their activities. The creation of an effective mechanism to prevent possible negative consequences from cyberattacks and cybercrimes in corporations today is a critically important task, without the solution of which the normal and effective functioning of the world economy and national security of the state is impossible.

As an innovative and conceptual mechanism for ensuring the information security of corporations' activities, a comprehensive mechanism is recommended, which includes innovative provision of corporations' activities and ensuring information security of corporations' activities to achieve an innovative level of the corporation's development and its development strategy.

Keywords: corporation; informatization; innovation; information security; provision.

Отримано: 11 червня 2022 р.
Прорецензовано: 16 червня 2022 р.
Прийнято до друку: 24 червня 2022 р.