СТРАТЕГІЧНІ ОРІЄНТИРИ ФОРМУВАННЯ КОРПОРАТИВНОЇ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

STRATEGIC GUIDELINES FOR FORMATION OF CORPORATE INFORMATION SECURITY POLICY

УДК 004.73056.5(045)
DOI: https://doi.org/10.32843/bses.72-28

Чубаєвський В.І.
к.політ.н., доцент,
доцент кафедри інженерії
програмного забезпечення
та кібербезпеки
Київський національний
торговельно-економічний університет

Chubaievskyi Vitaliy
Kyiv National University
of Trade and Economics

У статті науково обґрунтовано необхідність застосування комплексної системи захисту інформації корпоративного простору під час упровадження корпоративної політики інформаційної безпеки. Доведено доцільність зміни парадигми корпоративної політики шляхом визначення стратегічного підходу до формування єдиного цифрового корпоративного бізнес-простору. Урахування стратегічного підходу в умовах трансформаційних змін дало змогу визначити необхідність формування стратегічних орієнтирів розвитку корпорацій з урахуванням ключових викликів, як зумовлюють необхідність змін їхньої діяльності за такими напрямами: цифрові бізнес-стратегії, стратегії мінімізації інцидентів з інформаційною безпекою та стратегії організаційно-управлінського забезпечення перспектив розвитку інформаційної безпеки. Визначені стратегічні орієнтири виявили потребу в оновленому підході до систематизації видів корпоративних політик інформаційної безпеки, які б ураховували динаміку стратегічних змін напрямів діяльності корпорацій відповідно до ключових викликів сучасності.

Ключові слова: *інформаційні технології, ключові виклики, стратегічні зміни, стратегічні орієнтири, інформаційна безпека, корпоративна політика інформаційної безпеки.*

В статье научно обоснована необходимость применения комплексной системы защиты корпоративного пространства при внедрении корпоративной политики информационной безопасности. Доказана целесообразность смены парадигмы корпоративной политики путем определения стратегического подхода к формированию единого цифрового корпоративного бизнес-пространства. Учет стратегического подхода в условиях трансформационных изменений позволил определить необходимость формирования стратегических ориентиров развития корпораций с учетом ключевых вызовов современности, которые обуславливают необходимость изменений их деятельности по следующим направлениям: цифровые бизнес-стратегии, стратегии минимизации инцидентов с информационной безопасностью и стратегии организационно-управленческого обеспечения перспектив развития информационной безопасности. Выделенные стратегические ориентиры выявили потребность в обновлении подхода к систематизации видов корпоративных политик информационной безопасности, учитывающих динамику стратегических изменений направлений деятельности корпораций в соответствии с ключевыми вызовами современности.

Ключевые слова: *информационные технологии, ключевые вызовы, стратегические изменения, стратегические ориентиры, информационная безопасность, корпоративная политика информационной безопасности.*

In today's conditions of corporate development, the landscape of corporate information security issues has shifted from a narrowly focused technical issue to a strategic business priority. The main goal of corporate information security policy is to ensure business continuity and reduce losses by preventing and minimizing the consequences of security incidents. Corporate information security policy is an element of corporate governance and follows from the strategic requirements for risk management and corporate governance. Corporate information security should be implemented in accordance with business goals, which are characterized by a high level of dynamism in the conditions of the need for continuous consistent coordination between security policy and other areas of corporate business policy and strategies. Consistent coordination of information security policy can be achieved by converging corporate information security policy with other business policies of the organization within the strategic management cycle. Today there is an objective need to create a system of protection of corporate information systems and strengthen the national security of the country by including information security of the corporate sector in the system of corporate governance. Defining information security as one of the main requirements of the corporate governance system, it should be noted that it is a corporate tool to ensure sustainable, dynamic and balanced development of domestic corporations. The article scientifically substantiates the need to use a comprehensive system of information protection of corporate space in the implementation of corporate information security policy. The expediency of changing the paradigm of corporate policy by defining a strategic approach to the formation of a single digital corporate business space is proved. Taking into account the strategic approach in the conditions of transformational changes allowed to determine the need to form strategic guidelines for corporate development taking into account key challenges, as necessitating changes in their activities in the following areas: digital business strategies, security. The identified strategic guidelines revealed the need for an updated approach to the systematization of types of corporate information security policies, which would take into account the dynamics of strategic changes in the activities of corporations in accordance with the key challenges of today.

Key words: *information technologies, key challenges, strategic changes, strategic guidelines, information security, corporate information security policy.*

Постановка проблеми. У сучасних умовах розвитку корпорацій ландшафт питань забезпечення інформаційної безпеки корпорацій перемістився з вузькоспрямованого технічного питання до стратегічного пріоритетного завдання бізнесу. Головною метою корпоративної політики інформаційної безпеки є забезпечення безперервності бізнесу та зменшення збитків шляхом запобігання та мінімізації наслідків інцидентів безпеки.

Отже, сьогодні виникає об'єктивна необхідність створення системи захисту корпоративних інформаційних систем та зміцнення національної безпеки країни шляхом включення інформаційної безпеки корпоративного сектору до системи корпоративного управління. Визначаючи інформаційну безпеку однією з основних вимог системи корпоративного управління, слід зазначити, що вона є корпоративним інструментом забезпечення

стійкого, динамічного та збалансованого розвитку вітчизняних корпорацій.

Аналіз останніх досліджень і публікацій. Питання формування корпоративних політик інформаційної безпеки в умовах трансформаційних змін досліджували такі вітчизняні та зарубіжні вчені, як: І. Анікін [3], З. Валіулліна [7], В. Глова [3], О.В. Гордієнко [7], В. Домарєв [8], А. Страхарчук [9], О. Черевко [13], С. Парк [25], Т. Руіджхавер [25], У. Флорес [18], К.С. Хонг [23] та ін.

Постановка завдання. Метою статті є обґрунтування необхідності та доцільності зміни парадигми корпоративної політики інформаційної безпеки шляхом визначення стратегічного підходу до формування єдиного цифрового корпоративного бізнесу-простору Урахування стратегічного підходу в умовах трансформаційних змін дасть змогу визначити необхідність формування стратегічних орієнтирів розвитку корпорацій з урахуванням ключових викликів сучасності.

Виклад основного матеріалу дослідження. Питання формування ефективної корпоративної політики інформаційної безпеки в різних її аспектах досліджували багато вітчизняних та зарубіжних науковців. Але, незважаючи на значну кількість праць, слід констатувати факт відсутності уніфікованого термінологічного узагальнення політики інформаційної безпеки та механізмів її реалізації, що активізує дискусії науковців стосовно систематизації політики інформаційної безпеки та методичного інструментарію її впровадження як на рівні держави, так і на рівні корпорацій.

Стаття 17 Конституції України регламентує захист інформаційної безпеки нарівні із захистом суверенітету та територіальної цілісності України, що є найважливішою функцією держави та справою всього українського народу [1].

Відповідно до Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», поняття «інформаційна безпека» має таке визначення: «Стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого 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» [2]. Оскільки саме інформаційна система синтезує дані про стан та тенденції розвитку всіх інших систем діяльності корпорацій, вона водночас функціонує як відокремлений складник, так і у взаємодії з іншими елементами корпоративної системи, створюючи єдиний інформаційний корпоративний простір.

Аналізуючи сутність корпоративної політики інформаційної безпеки, слід зазначити, що більшість науковців розглядає її тільки через склад її компонентів, без виділення в окрему категорію вказаного терміна.

В. Домарєв та О. Гордієнко характеризують політику інформаційної безпеки як набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз [8, с. 103].

І. Анікін, В. Глова, А. Нігматулліна визначають політику інформаційної безпеки як набір норм, правил і практичних рекомендацій, що регламентують процес обробки інформації, виконання яких забезпечує захист від заданої множини загроз [3, с. 25]

На думку А. Страхарчука і В. Страхарчука, політика інформаційної безпеки – це набір законів, правил і практичних рекомендацій, на базі яких здійснюється керування, захист та розподіл критичної інформації в системі [10, с. 132].

Є. Бодюл пропонує під політикою інформаційної безпеки розуміти науково обґрунтовану систему поглядів на визначення основних напрямів, умов і порядку практичного вирішення завдань інформаційного захисту організацій та установ від протиправних дій [5].

За визначенням Ю. Хохлачової, політика інформаційної безпеки – це сукупність керівних принципів, правил, процедур фактичних прийомів, якими об’єкт керується у своїй діяльності [12, с. 25].

М. Бондаренко, О. Потій, І. Горбенко та ін. характеризують політику інформаційної безпеки як сукупність правових і морально-етичних норм, правил, адміністративних, організаційних заходів та технічних, програмних і криптографічних засобів, спрямованих на захист інформаційної інфраструктури організації від випадкового і навмисного втручання в процес її функціонування [6, с. 11].

На думку А. Нашинець-Наумової, політика інформаційної безпеки – це сукупність нормативних документів, які встановлюють порядок забезпечення безпеки інформації на конкретному підприємстві, а також висувають вимоги до підтримки цього порядку [11, с. 39].

Слід зазначити, що більшість вітчизняних науковців доводить необхідність застосування комплексної системи захисту інформації корпоративного простору під час упровадження корпоративної політики інформаційної безпеки.

З. Валіулліна та О. Черевко зазначають, що в умовах сучасних глобалізаційних процесів інформаційна безпека корпорацій є пріоритетним напрямом соціально-економічного розвитку держави. При цьому автори обґрунтовують необхідність упровадження в діяльність корпорацій заходів законодавчого, економічного, програмно-технічного та адміністративно-управлінського характеру, комплексний влив яких дасть змогу створити інформаційно безпечний корпоративний

простір [7, с. 35]. При цьому формування системи комплексного захисту інформаційних ресурсів повинно бути забезпечене, перш за все, за рахунок системи створення механізмів власного забезпечення, здатних реалізувати її функціонування не тільки в повсякденних умовах, а й у критичних ситуаціях [13].

Погоджуючись з вищезазначеними думками, А. Нашинець-Наумова відзначає необхідність застосування комплексу відповідних заходів також для проведення систематичного моніторингу стану інформаційної безпеки корпорацій та розроблення оптимальної моделі функціонування системи її забезпечення шляхом створення необхідних організаційно-економічних та правових механізмів формування розвитку і забезпечення ефективного використання інформаційних ресурсів корпорації [11, с. 60].

О. Жабинець під час розроблення політики інформаційної безпеки відзначає доцільність прийняття відповідних заходів, спрямованих на захист активів компаній від будь-якої зміни, розкриття чи знищення, а також із метою забезпечення конфіденційності, цілісності та доступності інформації [9, с. 25].

М. Шилов та І. Жевелєва акцентують увагу на необхідності впровадження в діяльність корпорацій комплексу заходів та засобів контролю, які б дали змогу здійснювати систематичне управління безпекою та ризиками [14, с. 135].

В. Бакай та В. Зима обґрунтовують думку про те, що в умовах глобалізації саме ефективна політика інформаційної безпеки є пріоритетним механізмом забезпечення системи економічної безпеки підприємства й економічної безпеки держави загалом. Водночас автори наголошують на тому, що саме політика забезпечення інформаційної безпеки є неодмінною умовою переходу на модель стійкого розвитку корпорацій, доводячи, що «у нових реаліях без належного захисту інформаційного середовища підприємства неможливо забезпечити його економічну безпеку» [4, с. 20].

Наведені вище підходи до визначення корпоративної політики інформаційної безпеки відображають погляди багатьох вітчизняних дослідників, але не враховують стратегічний підхід до феномену цього поняття.

Необхідність урахування саме стратегічного підходу до формування корпоративної політики інформаційної безпеки обґрунтовується тим, що сьогодні інформаційні технології відіграють пріоритетну роль у розвитку бізнесу, забезпечуючи гнучку адаптацію бізнес-структур до впровадження інновацій та формування потенціалу і розвитку їхніх конкурентних переваг.

Тому зміна парадигми корпоративної політики інформаційної безпеки для зміни її вектору від внутрішньоорієнтованого захисту інформації до стратегічного погляду, який ураховує міжорганізаційний рівень, є об'єктивно необхідною та доцільною. Зміна парадигми корпоративної політики шляхом визначення стратегічного підходу дасть змогу визначати акценти та сфокусуватися саме на впровадженні в діяльність корпорацій механізмів щодо захисту інформаційних ресурсів на користь тих стейкхолдерів, які приймають рішення та відповідальні за забезпечення ефективної політики інформаційної безпеки організації на стратегічному рівні.

У працях багатьох зарубіжних дослідників визначається, що збереження конфіденційності, цілісності та доступності інформаційних ресурсів є важливою вимогою для організації, як і потреба у життєздатній стратегії інформаційної безпеки в організаціях для полегшення передачі інформації на міжорганізаційному рівні [24, с. 66].

На думку Н. Бибе і В. Рао, стратегічна політика інформаційної безпеки визначається як «шаблон або план, який об'єднує основні цілі, політику та послідовність дій організації щодо інформаційної безпеки в єдине ціле» [15, с. 341]. Автори наголошують на необхідності узгодження оцінки зовнішніх інформаційних загроз із фінансово обґрунтованим комплексом внутрішніх контрзаходів, включаючи необхідні допоміжні політики та процедури. Отже, політика інформаційної безпеки розглядається як ключовий інструмент впливу на зовнішнє бізнес-середовище організації шляхом ретельного відбору засобів внутрішнього контролю.

С. Парк і Т. Руіджхавер визначають корпоративну політику інформаційної безпеки як «мистецтво вирішувати, як найкращим чином використовувати відповідні технології та заходи оборонної інформаційної безпеки, а також скоординовано розгортати та застосовувати їх до інформаційної інфраструктури корпорації проти внутрішніх та зовнішніх загроз, пропонуючи конфіденційність, цілісність та доступність за рахунок найменших зусиль і витрат» [25, с. 28].

Дослідження корпоративної політики інформаційної безпеки цими авторами доводить її міцний зв'язок з організаційним стратегічним планом корпорації. Саме стратегічна політика інформаційної безпеки дасть змогу корпораціям запобігти існуючим та потенційним загрозам інформаційним ресурсам у часі, просторі й у процесі прийняття управлінських рішень [28, с. 322].

К.С. Хонг та ін. стверджують, що саме врахування стратегічного підходу до формування корпоративної політики інформаційної безпеки дає змогу розширити її функціонал та зорієнтуватися на управління ризиками та надзвичайними ситуаціями [23, с. 246].

У. Флорес та інші зарубіжні вчені розглядають корпоративну політику інформаційної безпеки як динамічний процес забезпечення захисту корпо-

ративної інформації, який реалізується зацікавленими особами [18, с. 97].

Отже, корпоративна інформаційна політика інформаційної безпеки є ключовим елементом загальної бізнес-стратегії корпорації, який включає адекватну підтримку її стратегічного розвитку, згуртованість інформаційних систем і бізнесу та координацію зусиль з інформаційної безпеки.

Функціонування сучасних корпоративних структур в умовах динамічного бізнес-середовища змушує перманентно враховувати та приймати нові технології. Саме технологічний вплив зумовлює необхідність формування стратегічного вектору розвитку корпорацій з урахуванням ключових викликів, що зумовлюють необхідність змін напрямів їхньої діяльності (табл. 1).

Корпоративні структури швидко впроваджують цифрові бізнес-стратегії, які характеризуються високим рівнем технологічного розгортання. Наприклад, корпоративне використання хмарних сервісів, блокчейну, штучного інтелекту, Інтернету речей, великих даних, мобільних і соціальних мереж. Така тенденція призвела до всебічного вбудовування інформаційних технологій у бізнес корпорацій [25, с. 270]. Об'єктивно сформований поточний технологічний бізнес-клімат повністю нівелював дистанцію між традиційним фізичним і новим цифровим світом, створив єдиний простір інформаційних технологій та бізнесу, перетворив безпеку з ізольованої проблеми на стратегічний напрям корпоративної політики інформаційної безпеки, який вимагає розроблення та впровадження відповідних регулюючих механізмів.

По-друге, через усебічне впровадження інформаційних технологій у бізнес інциденти з інформаційною безпекою, що викликають порушення стійкості функціонування корпорацій, безпосередньо впливають на прогресивність розвитку бізнесу корпорацій.

Кібератаки обмежують, перш за все продуктивність діяльності корпорацій, їхні інноваційні можливості та конкурентні переваги. Це призводить до зменшення кола бізнес-партнерів, фінансових та репутаційних збитків [22, с. 87].

Окрім того, зарубіжні науковці виявили кореляцію між інцидентами інформаційної безпеки та ефективністю діяльності корпорацій компаній [19, с. 797]. Факт виникнення порушення інформаційної безпеки негативно впливає на ринкову вартість, коливається від 1% до 2,1% [20, с. 405]. Зростання впливу кібератак на безпеку та ринкову вартість корпорацій змушує керівників корпорацій здійснювати постійний пошук альтернативних механізмів їх мінімізації.

По-третє, цифровізація вимагає від організацій перейти на стратегічні міжорганізаційні перспективи забезпечення безпеки бізнесу корпорацій. Постійні порушення інформаційної безпеки підвищують розумні очікування клієнтів корпорацій щодо розроблення та впровадження заходів для захисту їхньої безпеки і конфіденційності. Запорукою збереження та відтворення потенціалу цільової аудиторії корпорацій є формування нормативно-правової бази, що регламентує та забезпечує права всіх стейкхолдерів бізнесу, таким чином, ще більше стимулює ці очікування.

Окрім цього, слід зазначити, що в умовах сучасного цифрового середовища корпорації функціонують як цифровий ланцюг поставок, а не як окремі бізнес-одиниці [16, с. 171]. Такий механізм їх функціонування зумовлює виникнення ризиків інформаційної безпеки за межами корпорацій, розширюючи завдання щодо розроблення відповідного методичного інструментарію формування ефективної корпоративної політики інформаційної

Таблиця 1

Стратегічні напрями діяльності корпорацій

Напрями діяльності, що потребують стратегічних змін	Ключові виклики
Цифрові бізнес-стратегії	Упровадження інформаційної безпеки в бізнес
	Відсутність розриву між фізичним і цифровим світом
	Безпека – це пріоритетний стратегічний напрям комплексного вирішення питань бізнесу
Стратегії мінімізації інцидентів з інформаційною безпекою	Залучення керівництва до перманентного вирішення питань щодо мінімізації інцидентів із безпекою
	Зростання безпосереднього впливу кібератак на бізнес, що вимагає постійного пошуку альтернативних механізмів управління інформаційною безпекою
Стратегії організаційно-управлінського забезпечення перспектив розвитку інформаційної безпеки	Кібератаки обмежують інноваційні можливості та продуктивність корпорації, зменшуючи їхні конкурентні переваги
	Перехід від внутрішньої до міжорганізаційної взаємодії
	Транскордонні ризики безпеки
	Збільшення довіри до діяльності корпорацій шляхом підвищення рівня безпеки та конфіденційності

Джерело: авторська розробка

безпеки, яка має бути зосереджена на створенні прозорого міжорганізаційного захисту інтересів усіх зацікавлених осіб.

Висновки з проведеного дослідження. Таким чином, політика інформаційної безпеки корпорацій є елементом корпоративного управління і випливає зі стратегічних вимог до управління ризиками та корпоративного управління. Інформаційна безпека корпорацій має бути реалізована відповідно до бізнес-цілей, які характеризуються високим рівнем динамічності за умов необхідності безперервного послідовного узгодження між політикою безпеки та іншими напрямами корпоративної бізнес-політики та стратегіями.

Послідовне узгодження політики інформаційної безпеки може бути досягнуто шляхом конвергенції корпоративної політики інформаційної безпеки з іншими бізнес-політиками

Стратегічні зміни, зумовлені впровадженням інформаційних технологій та формуванням єдиного цифрового корпоративного бізнес-простору, виявили потребу в оновленому підході до розроблення методичних засад систематизації видів корпоративних політик інформаційної безпеки, які б ураховували динаміку стратегічних змін напрямів діяльності корпорацій відповідно до ключових викликів сучасності.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Конституція України : Основний Закон України від 28.06.1996 № 254к/96-ВР. URL: http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 10.12.2021).

2. Zakon Ukrainy «Pro Osnovni zasady rozvytku informatsiinoho suspilstva v Ukraini na 2007–2015 roky». URL: http://zakon.rada.gov.ua (дата звернення: 15.12.2021).

3. Аникин И.В., Глова В.И., Нигматуллина А.Н. Методы и средства защиты компьютерной информации : учебное пособие. Казань : Казан. гос. техн. ун-т, 2008. 212 с.

4. Бакай В.Й., Зима В.М. Нові виклики та особливості створення системи інформаційної безпеки підприємства. *Вісник Хмельницького національного університету*. 2020. № 5. С. 19–22.

5. Бодюл Є.М. Інформаційна безпека банку. *Протидія злочинам, які вчиняються з використанням комп'ютерних мереж* : тези доповідей Міжнародної науково-практичної конференції, м. Севастополь, 1–2 жовтня 2010 р. Суми : ДВНЗ «УАБС НБУ», 2010. С. 135–137.

6. Визначення та обґрунтування суті політики інформаційної безпеки / М.Ф. Бондаренко, О.В. Потій, Ю.І. Горбенко та ін. *Радиотехника*. 2003. № 134. С. 9–25.

7. Валіулліна З.В. Інформаційна безпека корпоративної економіки в умовах глобалізаційних процесів. *Вісник Дніпропетровського університету. Серія «Менеджмент інновацій»*. 2016. Вип. 6. С. 34–41.

8. Домарєв В.В., Гордієнко О.В. Обґрунтування основних функцій системи управління інформаційною безпекою. *Вісник Державного університету інформаційно-комунікаційних технологій*. 2012. Т. 10. № 2. С. 102–104.

9. Жабинець О.Й. Політика інформаційної безпеки страхових компаній: українські реалії та досвід США. *Проблеми економіки*. 2014. № 4. С. 22–27.

10. Страхарчук А.Я., Страхарчук В.П. Інформаційні системи і технології в банках : навчальний посібник. Київ : Знання, 2010. 515 с.

11. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. Київ : Гельветика, 2017. 168 с.

12. Хохлачова Ю. Політика інформаційної безпеки об'єкта. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2012. № 2(24). С. 23–29.

13. Черевко О.В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту. *Ефективна економіка.* 2014. № 5. URL: http://www.economy.nayka.com.ua/?op=1&z=3304 (дата звернення: 17.12.2021).

14. Шилов М.С., Жевелєва І.С. Актуальні проблеми управління інформаційною безпекою держави. *Збірник тез наукових доповідей науково-практичної конференції*, м. Київ, 26 березня 2021 р. Київ : НА СБУ, 2021. С. 325.

15. Beebe, N.L., and Rao, V.S. (2010) Improving Organizational Information Security Strategy Via MesoLevel Application of Situational Crime Prevention to the Risk Management Process. *Communications of the Association for Information Systems* (26:17). P. 329–358.

16. Büyüközkan, G. and Göçer, F. (2018), "Digital supply chain: literature review and a proposed framework for future research", *Computers in Industry,* vol. 97, pp. 157–177.

17. Carcary, M., Renaud, K., McLaughlin, S. and O'Brien, C. (2016), "A framework for information security governance and management", IT Professional, vol. 18, no. 2, pp. 22–30. DOI: https://doi.ieeecomputersociety.org/10.1109/MITP.2016.27.

18. Flores, W.R., Antonsen, E., and Ekstedt, M. (2014) Information Security Knowledge Sharing in Organizations: Investigating the Effect of Behavioral Information Security Governance and National Culture. Computers & Security (43), pp 90–110.

19. Georg, L. (2017) Information security governance: pending legal responsibilities of non-executive boards. *Journal of Management and Governance*, vol. 21, no. 4, pp. 793–814. DOI: 10.1007/s10997- 016-9358-0.

20. Gillon, K., Branz, L., Culnan, M.J., Dhillon, G., Hodgkinson, R. and MacWillson, A. (2011) Information security and privacy-rethinking governance models. *Communications of the Association for Information Systems*. Vol. 28. P. 33. DOI: 10.17705/1CAIS.02833.

21. Goel, S. and Shawky, H.A. (2009) Estimating the market impact of security breach announcements on firm values. *Information and Management*, vol. 46, no. 7, pp. 404–410. DOI: 10.1016/j.im.2009.06.005.

22. Hasbini, M.A., Eldabi, T. and Aldallal, A. (2018), "Investigating the information security management role in smart city organisations", *World Journal of Entrepreneurship, Management and Sustainable Development*, vol. 14, no. 1, pp. 86–98, DOI: 10.1108/WJEMSD07-2017-0042.

23. Hong, K.-S., Chi, Y.-P., Chao, L., and Tang, J.-H. (2003). "An Integrated System Theory of Information Security Management," *Information Management & Computer Security* (11:5), pp. 243–248

24. Kim, S.H., Wang, Q.-H., and Ullrich, J.B. (2012). "A Comparative Study of Cyberattacks," *Communications of the ACM* (55:3), p. 66.

25. Mishchuk I., Riabykina Ye., Ushenko N., Hamova O., Tkachenko S., Yastremska N. (2022). "Intellectual Capital as a Factor Forming Economic Security of Enterprises in Society 5.0 ," *WSEAS Transactions on Business and Economics,* vol. 19, pp. 269–277.

26. Park, S., and Ruighaver, T. (2008). "Strategic Approach to Information Security in Organizations," ICISS. *International Conference on Information Science and Security*, 2008: IEEE, pp. 26–31

27. Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016), "Information security management needs more holistic approach: a literature review", *International Journal of Information Management*, vol. 36, no. 2, pp. 215–225. DOI: 10.1016/j.ijinfomgt.2015.11.009.

28. Tereshchenko E., Shkolenko O., Kosmidailo I, Kalina I., Shuliar N. (2021). Formation of an effective risk management system at the enterprise. *Collection of scientific papers: «Financial and credit activity: problems of theory and practice».* Vol 1 (36), pp. 320–329. DOI: 10.18371/fcaptp.v1i36.227924.

REFERENCES:

1. Konstitutsiia Ukraïni (1996): Osnovnii Zakon Ukraïni [Constitution of Ukraine: Basic Laws of Ukraine] № 254к/96-VR. URL: http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (accessed 10 December 2021).

2. Zakon Ukrainy «Pro Osnovni zasady rozvytku informatsiinoho suspilstva v Ukraini na 2007–2015 roky» [Law of Ukraine "On the main measures for the development of the information society in Ukraine for 2007–2015"]. URL: http://zakon.rada.gov.ua (accessed 15 December 2021). (in Ukrainian)

3. Anikin I.V., Glova V.I., Nigmatullina A.N. (2008) Metody i sredstva zashchity kompiuternoi informatsii [Methods and means of protection of computer information]. Textbook. Kazan: Kazan Publishing House. state tech. un-ty. 212 p. (in Russian)

4. Bakai V.Y., Zyma V.M. (2020) Novi vyklyky ta osoblyvosti stvorennia systemy informatsiinoi bezpeky pidpryiemstva. [New challenges and features of creating an information security system of the enterprise]. *Bulletin of Khmelnytsky National University,* no. 5, pp. 19–22. (in Ukrainian)

5. Bodiul Ye.M. (2010) Information security bank Informatsiina bezpeka banku: protydiia zlochynam, yaki vchyniaiutsia z vykorystanniam kompiuternykh merezh. [Information security of the bank. Combating crimes committed with the use of computer networks]. Abstracts of reports of the International scientific-practical conference (Sevastopol, October 1–2, 2010). *State Higher Educational Institution "Ukrainian Academy of Banking of the National Bank of Ukraine".* Sumy: SHEI "UABS NBU", pp. 135–137. (in Ukrainian)

6. Bondarenko M.F., Potii O.V., Horbenko Yu.I. ta in. (2003) Vyznachennia ta obgruntuvannia suti polityky informatsiinoi bezpeky [Definition and substantiation of the essence of information security policy]. *Radio engineering*, vol. 134, pp. 9–25. (in Ukrainian)

7. Valiullina Z.V. (2016) Informatsiina bezpeka korporatyvnoi ekonomiky v umovakh hlobalizatsiinykh protsesiv [Information security of the corporate economy in the context of globalization processes]. *Bulletin of Dnipropetrovsk University. Series: Innovation Management.* Issue 6, pp. 34–41. (in Ukrainian)

8. Domariev V.V., Hordiienko O.V. (2012) Obgruntuvannia osnovnykh funktsii systemy upravlinnia informatsiinoiu bezpekoiu [Substantiation of the main functions of the information security management system]. *Bulletin of the State University of Information and Communication Technologies*. T. 10, vol. 2, pp. 102–104. (in Ukrainian)

9. Zhabynets O.Y. (2014) Polityka informatsiinoi bezpeky strakhovykh kompanii: ukrainski realii ta dosvid SShA.[Information security policy of insurance companies: Ukrainian realities and USA experience]. *Problems of economics*, vol. 4, pp. 22–27. (in Ukrainian)

10. Strakharchuk A.Ja., Strakharchuk V.P. (2010) Informacijni systemy i tekhnologhiji v bankakh [Information systems and technologies in banks]. Textbook. Kyiv: UBS NBU: Knowledge. 515 p. (in Ukrainian)

11. Nashynets-Naumova A.Yu. (2017) Informatsiina bezpeka: pytannia pravovoho rehuliuvannia. [Information security: issues of legal regulation]. Kyiv: Helvetica Publishing House. 168 p. (in Ukrainian)

12. Khokhlachova Yu. (2012) Polityka informatsiinoi bezpeky obiekta [Object information security policy]. *Legal, regulatory and metrological support of the information protection system in Ukraine,* vol. 2 (24), pp. 23–29. (in Ukrainian)

13. Cherevko O.V. (2014) Teoretychni zasady poniattia informatsiinoi bezpeky ta klasyfikatsiia zahroz systemi informatsiinoho zakhystu [Theoretical foundations of the concept of information security and classification of threats to the information security system]. *Effective Economy*, vol. 5. URL: http://www.economy.nayka.com.ua/?op=1&z=3304 (accessed 17 December 2021). (in Ukrainian)

14. Shylov M.S., Zhevelieva I.S. (2021) Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy [Actual problems of information security management of the state]. A collection of abstracts of scientific reports of the scientific-practical conference (Kyiv, March 26, 2021). Kyiv: NA SBU, p. 325. (in English)

15. Bakai V.Y., Zyma V.M. (2020) Novi vyklyky ta osoblyvosti stvorennia systemy informatsiinoi bezpeky pidpryiemstva. [New challenges and features of creating an information security system of the enterprise]. *Bulletin of Khmelnytsky National University,* vol. 5, pp. 19–22. (in English)

16. Beebe, N.L., and Rao, V.S. (2010) "Improving Organizational Information Security Strategy Via MesoLevel Application of Situational Crime Prevention to the Risk Management Process," *Communications of the Association for Information Systems* (26:17), pp. 329–358. (in English)

17. Büyüközkan, G. and Göçer, F. (2018), "Digital supply chain: literature review and a proposed frame-

work for future research", *Computers in Industry,* vol. 97, pp. 157–177. (in English)

18. Carcary, M., Renaud, K., McLaughlin, S. and O'Brien, C. (2016), "A framework for information security governance and management", *IT Professional,* vol. 18 no. 2, pp. 22–30. DOIt: https://doi.ieeecomputersociety.org/10.1109/MITP.2016.27. (in English)

19. Flores, W.R., Antonsen, E., and Ekstedt, M. (2014). "Information Security Knowledge Sharing in Organizations: Investigating the Effect of Behavioral Information Security Governance and National Culture," *Computers & Security* (43), pp 90–110. (in English)

20. Georg, L. (2017), "Information security governance: pending legal responsibilities of non-executive boards", *Journal of Management and Governance*, vol. 21, no. 4, pp. 793–814, DOI: 10.1007/s10997-016-9358-0. (in English)

21. Goel, S. and Shawky, H.A. (2009), "Estimating the market impact of security breach announcements on firm values", *Information and Management,* vol. 46, no. 7, pp. 404–410, DOI: 10.1016/j.im.2009.06.005. (in English)

22. Hasbini, M.A., Eldabi, T. and Aldallal, A. (2018), "Investigating the information security management role in smart city organisations", World Journal of Entrepreneurship, Management and Sustainable Development, vol. 14, no. 1, pp. 86–98. DOI: 10.1108/WJEMSD07-2017-0042. (in English)

23. Hong, K.-S., Chi, Y.-P., Chao, L., and Tang, J.-H. (2003). "An Integrated System Theory of Information Security Management," *Information Management & Computer Security* (11:5), pp. 243–248. (in English)

24. Kim, S.H., Wang, Q.-H., and Ullrich, J.B. (2012). "A Comparative Study of Cyberattacks," *Communications of the ACM* (55:3), p 66. (in English)

25. Mishchuk I., Riabykina Ye., Ushenko N., Hamova O., Tkachenko S., Yastremska N. (2022). "Intellectual Capital as a Factor Forming Economic Security of Enterprises in Society 5.0 ," *WSEAS Transactions on Business and Economics*, vol. 19, pp. 269–277.

26. Park, S., and Ruighaver, T. (2008). "Strategic Approach to Information Security in Organizations," ICISS. *International Conference on Information Science and Security,* 2008: IEEE, pp. 26–31. (in English)

27. Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016). "Information security management needs more holistic approach: a literature review", International Journal of Information Management, vol. 36, no. 2, pp. 215–225, DOI: 10.1016/j.ijinfomgt.2015.11.009. (in English)

28. Tereshchenko E., Shkolenko O., Kosmidailo I, Kalina I., Shuliar N. (2021). Formation of an effective risk management system at the enterprise. Collection of scientific papers: «Financial and credit activity: problems of theory and practice», vol 1 (36), pp. 320–329. DOI: 10.18371/fcaptp.v1i36.227924. (in Ukrainian)