ЕКОНОМІЧНИЙ ПРОСТІР

Chubaievskyi V. Svitova praktyka upravlinnja podijamy informacijnoi' bezpeky korporacij. *Zovnishnja torgivlja: ekonomika, finansy, pravo*. 2022. № 6. S. 73-82. Serija. Ekonomichni nauky. https://doi.org/10.31617/3.2022(125)05

УДК 339.9:004.056]:005.34

DOI: 10.31617/3.2022(125)05

ЧУБАЄВСЬКИЙ Віталій,
к. політ. н., доцент, доцент кафедри інженерії, програмного забезпечення та кібербезпеки Державного торговельно-економічного університету
вул. Кіото, 19, м. Київ, 02156, Україна
ORCID: 0000-0001-8078-2652
chubaievskyi_vi@knute.edu.ua

CHUBAIEVSKYI Vitaliy,
PhD (Politics), Associate Professor
Associate Professor of the Engineering Department of software and cyber security
State University of Trade and Economics
19, Kyoto St., Kyiv, 02156, Ukraine
ORCID: 0000-0001-8078-2652
chubaievskyi_vi@knute.edu.ua

СВІТОВА ПРАКТИКА УПРАВЛІННЯ ПОДІЯМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАЦІЙ

Вступ. *Накопичені у сфері захисту інформації досвід, та нові вимоги щодо побудови політики інформаційної безпеки компаній дали змогу виробити досить ефективні рекомендації щодо побудови системи управління інформаційною безпекою.*

Проблема. *Центральним процесом у системі управління інформаційною безпекою корпорацій є процес «Управління подіями». Тільки компетентна організація цього процесу може забезпечити належний рівень усієї послідовності етапів ефективного функціонування системи захисту корпоративної інформації, що охоплює всі дії протягом усього життєвого циклу події інформаційної безпеки; від планування, навчання та підвищення обізнаності до виявлення, реагування та навчання на подіях інформаційної безпеки.*

Метою *статті є теоретико-методичне обґрунтування доцільності запровадження процесу Управління подіями інформаційної безпеки в контексті аналізу світової практики системи захисту корпоративної інформації.*

Методи. *У ході дослідження використано методи системного підходу, теоретичне узагальнення та порівняння, аналіз і синтез. Інформаційною базою є власні дослідження автора, міжнародні стандарти інформаційної безпеки серії ISO/IEC 2700x, публікації в наукових виданнях та інтернет-ресурси.*

GLOBAL PRACTICE OF CORPORATE INFORMATION SECURITY EVENTS MANAGEMENT

Introduction. *The accumulated experience in the field of information protection, as well as new requirements for the construction of the information security policy of companies allowed to develop quite effective recommendations for the construction of the information security management system.*

Problem. *The central process in the information security management system of corporations is the «Event Management» process. Only a competent organization of this process can ensure the proper level of the entire sequence of stages of the effective functioning of the corporate information protection system, covering all actions during the entire life cycle of an information security event; from planning, training and raising awareness to detection, response and training at information security events.*

The aim *of the article is theoretical and methodological substantiation of the expediency of introducing the Information Security Event Management process in the context of the analysis of the global practice of the corporate information protection system.*

Methods. *The following methods were used in the course of research: the methods of the system approach, theoretical generalization and comparison, analysis and synthesis. The information base is the author's own research, international standards of information security of the ISO/IEC 2700x series, publications in scientific editions and Internet resources.*

Дослідження виконано у рамках держбюджетної теми: «Цифрова трансформація торговельно-економічної та туристичної систем України» (номер державної реєстрації 0121U112231).

Результати. *У рамках дослідження проаналізовано два найефективніші варіанти (США та Європа) організації процесу Управління подіями. Проведений аналіз дав змогу виявити особливості організації кожного процесу, його переваги та недоліки, довів необхідність формування комплексного підходу до організації процесів.*

Обґрунтовано, що комплексний підхід до організації процесу Управління подіями має враховувати взаємопов'язаність з іншими процесами управління та бути гармонізований з міжнародними стандартами інформаційної безпеки.

Впровадження цього алгоритму дає змогу мінімізувати потенційні ризики, пов'язані з можливими втратами інформаційних ресурсів корпорації. А отже, й мінімізує потенційну економічну шкоду, що викликано недотриманням політики інформаційної безпеки корпорації.

Висновки. *Проведені дослідження дають можливість на практиці заповнити потенційні прогалини інформації під час створення системи управління інформаційною безпекою корпорацій. Додатковою перевагою запропонованого рішення є можливість задіяння цього підпроцесу як незалежного, що спрощує процедуру управління інформаційною безпекою корпорації загалом і сприяє зниженню витрати на її побудову.*

Ключові слова: інформаційна безпека, інциденти інформаційної безпеки, міжнародні стандарти інформаційної безпеки, система управління інформаційною безпекою, управління подіями інформаційної безпеки.

Results. *Within the framework of this study, the two most effective options (USA and Europe) for the organization of the Event Management process were analyzed. The conducted analysis made it possible to identify the peculiarities of the organization of each process, its advantages and disadvantages, proved the need for the formation of a comprehensive approach to the organization of processes.*

It is justified that a comprehensive approach to the organization of the Event Management process should take into account the interconnection with other management processes and be harmonized with international information security standards.

The implementation of this algorithm makes it possible to minimize the potential risks associated with the possible loss of information resources of the corporation. And, therefore, minimizes the potential economic damage caused by non-compliance with the corporation's information security policy.

Conclusions. *The conducted research makes it possible to practically fill potential information gaps when creating a system for managing information security of corporations. An additional advantage of the proposed solution is the possibility of using this sub-process as an independent one, which simplifies the procedure of managing information security of the corporation as a whole and contributes to reducing the cost of its construction.*

Keywords: informational security; information security incidents; international information security standards; information security management system; management of information security events.

JEL Classification: M11, D29, G34.

Конфлікт інтересів: Автор заявляє, що він не має фінансових чи нефінансових конфліктів інтересів щодо цієї публікації; не має відносин з державними органами, комерційними або некомерційними організаціями, які могли б бути зацікавлені у поданні цієї точки зору. З огляду на те, що автор працює 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 і редакторів) приймалося тими членами редколегії, які не пов'язані з цією установою.

Вступ. Від появи спочатку інформаційних систем, а потім корпоративних інформаційних системи проблема захисту інформації в них не втрачає актуальності. Свідченням цього є масштабні кібернетичні атаки, що прокотилися Україною та світом за останній рік [1; 2].

Накопичений у сфері захисту інформації досвід, а також нові вимоги щодо побудови політики інформаційної безпеки компаній дали змогу виробити досить ефективні рекомендації щодо побудови системи управління інформаційною безпекою. Причому сьогодні система управління інформаційною безпекою (СУІБ) інтегрує окремі, часто розрізнені заходи, спрямовані на забезпечення захисту інформації та інформаційної безпеки (ІБ) компанії. Ландшафт наявних загроз досить складний з великою різноманітністю зловмисників. Попри те, що організації реалізують заходи політики інформаційної безпеки та впроваджують

комплексні інструменти перманентного моніторингу і контролю, час від часу виникають нові вразливості та інциденти ІБ. Відтак організаціям потрібні плани та процедури для вирішення інцидентів інформаційної безпеки. Наявність в організації можливостей реагування на інциденти ІБ може допомогти їм швидко їх виявити, мінімізувати втрати та руйнування.

Проблема. Центральним процесом у СУІБ корпорацій є процес «Управління подіями». Тільки компетентна організація цього процесу може забезпечити належний рівень усієї послідовності етапів ефективного функціонування системи захисту корпоративної інформації, що охоплює всі дії протягом усього життєвого циклу події інформаційної безпеки – від планування, навчання та підвищення обізнаності до виявлення, реагування та навчання на подіях ІБ. Отже, сьогодні у корпорацій виникає об'єктивна необхідність розробки ефективної системи управляння подіями їхньої інформаційної безпеки.

Аналіз останніх досліджень і публікацій. Питанням побудови ефективної СУІБ компанії присвячено чимало досліджень. Однак варто зауважити, що низка вітчизняних і закордонних авторів, зокрема В. Хох, Е. Мелешко, О. Смірнов, А. Габріель, Т. Хоппе, А. Паства, С. Сова, С. Бхат, Р. Манадхата та інші [3–7] по-різному трактують термін «подія» у СУІБ. Таке «різночитання» створює складнощі у роботі аналітиків інформаційної безпеки корпорацій, передусім на рівні термінології. Крім того, у працях зазначених авторів не враховано те, що в ході реалізації процесів, пов'язаних з управлінням подіями, аналітика або аудитора ІБ спочатку цікавить факт запису про подію, що відбулася. Такий запис може бути фіксований в системі збору даних служби ІБ корпорації. Додатково фіксуються пов'язані події та стани системи захисту корпоративної інформації, наприклад, може йтися про підвищені рівні завантаження процесорів (або ядер) серверів, нетипові встановлені мережеві з'єднання [8] тощо. Наведені приклади також є подіями. Однак здебільшого дослідження з управління ІБ [8–12] подібним подіям не приділяють належної уваги.

Проте звужувати визначення «події», коли йдеться про забезпечення інформаційної безпеки корпорації, недоцільно – це може спричинити фактичне дублювання подій та активностей, що своєю чергою породжує неефективне використання ресурсів сторін захисту корпоративної інформаційної системи. І що найважливіше, може призвести до ситуації, коли важливі події в контексті ІБ можуть бути втрачені з поля зору аналітика системи захисту корпоративної інформації. Система управління подіями інформаційної безпеки корпорацій стає центральною платформою сучасних операційних центрів захисту корпоративної інформації, корелює ці події та надає синтетичні

перегляди сповіщень для обробки загроз і звітування про стан інформаційної безпеки.

Метою дослідження є теоретико-методичне обґрунтування доцільності запровадження процесу «Управління подіями» інформаційної безпеки в контексті аналізу світової практики системи захисту корпоративної інформації.

Методи. Для досягнення поставленої мети використано методи системного підходу, теоретичного узагальнення та порівняння, аналізу й синтезу. Інформаційною базою є власні дослідження автора, міжнародні стандарти інформаційної безпеки серії *ISO*/*IEC* 2700*x*, публікації в наукових виданнях та інтернет-ресурси.

Результати дослідження. У міру інтеграції України та її суб'єктів господарської діяльності до глобального міжнародного ринку українські компанії як методологічну основу побудови СУІБ застосовують стандарти серії *ISO*/*IEC* 2700*x* [13; 14].

Проте в низці випадків таке формування системи захисту корпоративної інформації на основі *ISO*/*IEC* 2700*x* не враховує особливостей Управління подіями у вітчизняних компаніях, оскільки міжнародна практика побудови СУІБ компаній насамперед спирається на процес Управління інцидентами. Утім багато фахівців в області ІБ компаній вважають, що Управління подіями є менш значущим фактором. Попри те, що пріоритет за побудови ефективної СУІБ відданий винятково Управлінню інцидентами, можна не зважати на цю обставину. Але лише процес Управління інцидентами не може втілити ефективний проактивний підхід у рамках надання *IT*-послуг та системи захисту корпоративної інформації, відтак не забезпечує максимально високого рівня інформаційної безпеки компанії.

Обмежена увага до впровадження процесу Управління інцидентами у компаніях найчастіше є наслідком відсутності стандартизованої та загальновизнаної методології. Причому ця методологія має бути адаптована до корпоративної політики інформаційної безпеки. Складності вирішення цього завдання обумовлені насамперед тими обсягами та трудомісткістю підготовчих робіт, яку варто провести аналітикам ІБ компанії. Причому чим більший масштаб компанії, тим більше параметрів необхідно врахувати. Параметри, що враховуються, можуть стосуватися як організаційного, так і технічного рівнів інформаційної системи або корпоративної інформаційної системи.

У рамках цього дослідження проаналізовано та детально порівняно два найефективніші варіанти організації процесу Управління подіями: стандарт *NIST SP* (*The National Institute of Standards and Technology*, США) 800-92 та методологія *ITIL* (*Information Technology Infrastructure Library*, *EC*) [10].

У стандарті *NIST SP* 800-92 регулюються питання управління логами (*Log Management*). У цьому документі лог (*Log*) сприймається як запис, відповідний певній події у системі. Під системою розуміється, наприклад, корпоративна інформаційна система чи мережа компанії. За своїми цілями у контексті трактування про опис лога можна говорити як про опис Управління подією. Своєю чергою у методології *ITIL* аналізується комплекс процесів СУІБ. Зокрема розглянуто й питання Управління подіями [10].

У *таблиці* наведено детальне порівняння даних документів та визнаних світових практик з виділенням їх сильних і слабких сторін.

Таблиця

Світові практики організації процесу Управління подіями в системі управління інформаційною безпекою

Нормативний документ	Область дії	Ключові переваги та особливості	Недоліки
Стандарт *NIST SP* 800-92	Федеральні агенції США	Виділення пріоритетних логів; встановлення політиками та процедурами управління логами; створення та підтримання захищених інфраструктур управління логами; проведення заходів, пов'язаних із навчанням персоналу; моніторинг статусу ведення подій стосовно всіх джерел подій; моніторинг ротації подій; ведення архіву; контроль життєвого циклу системи обліку логів; забезпечення синхронізації подій; гнучке налаштування процедур фіксації логів; документування та складання звітності	Непослідовність під час викладу процесних аспектів
Методологія *ITIL*	Будь-які компанії чи організації	Визначення ключових активностей процесу Управління подіями; реєстрація подій; запис подій	Не враховано: практичні аспекти реалізації сучасних *IT*-інфраструктур компаній; особливості корпоративних інформаційних систем та контекст обробки подій, особливо в рамках життєвого циклу корпорацій

Джерело: складено автором за [5; 7; 9; 11].

За результатами аналізу провідних світових стандартів, методик, теоретичних та практичних досліджень [5; 7; 9; 11] можна зробити висновок, що такі документи не мають структурованого опису процесу Управління подіями, яке апріорі містить принципи безперервного вдосконалення у послідовності: планування (*Plan*) – реалізація (*Do*) – перевірка (*Check*) – дія (*Act*) [4; 5]. Крім того, здебільшого у розглянутих теоретичних працях не враховано найважливіші аспекти реалізації сучасних *IT*-інфраструктур компаній, особливості сучасних бізнес-процесів та обробки подій, що реалізуються у межах їхнього життєвого циклу.

Відтак потрібно сформувати комплексний підхід до організації процесів Управління подіями. Цей комплексний підхід повинен враховувати взаємопов'язаність з іншими процесами управління. Крім того, він має бути гармонізований зі стандартами *ISO*/*IEC* 2700*x*.

Удосконалення процесів управління ІБ передбачає необхідність урахування всієї сукупності принципів управління. Очевидно, що ці принципи беруть до уваги й особливості таких об'єктів: «інформаційна безпека»; «необхідність запобігання інцидентам»; «необхідність ослаблення інцидентів».

За традиційним підходом проблема підвищення рівня інформаційної безпеки компанії вирішується шляхом збільшення витрат на систему захисту корпоративної інформації. Це здебільшого сприяє зниженню рівня ризиків, пов'язаних з втратою інформації. Такий підхід, з погляду математичного моделювання процесів забезпечення корпоративної ІБ, базується на пошуку та обґрунтуванні оптимальних значень показників ризику втрати інформації, а також на пошуку відповідних значень мінімальних витрат на побудову ефективної системи ІБ компанії.

Якщо виходити з припущення, що підхід до побудови системи управління інформаційною безпекою має бути системним, то в сучасних реаліях (зміна ландшафту кібернетичних загроз, збільшення складності сценаріїв кібернетичних атак) акцент варто робити на адаптивності та інваріантності способів реалізації інфраструктурних рішень ІБ компанії.

Впровадження інформаційних технологій у процеси управління ІБ і зокрема в організацію процесів Управління подіями інформаційної безпеки компаній сприяє недопущенню потенційно можливих втрат. Попри наукової праці [2; 5; 7; 8; 10; 14] у рамках побудови СУІБ компанії запропоновано доповнення до способу організації процесу Управління подіями (*рисунок*).

Алгоритм адаптивного процесу
Управління подіями інформаційної безпеки корпорацій

Джерело: доповнено автором за [2; 5; 7; 8; 10; 14].

На відміну від наявної практики запропоновані доповнення дають змогу враховувати, що: не всі події реєструються; не всі ті події, які зареєстровані, відправляються на обробку до системи класу *SIEM* (*Security information and event management*) [6] або *SIP* (*Security event management*) [13]; обробка подій може породжувати нові події.

Запропонований на *рисунку* алгоритм адаптивного процесу Управління подіями дає можливість врахувати особливості, пов'язані з: визначенням політики Управління подіями для корпоративних інформаційних систем; забезпеченням інфраструктурних рішень щодо Управління подіями; обробкою подій у межах їхнього життєвого циклу; контролем інфраструктурних рішень щодо Управління подіями; контролем політики Управління подіями; у разі потреби – з корекцією інфраструктурних рішень щодо Управління подіями.

Доречно зауважити, що підпроцес «Обробка та аналіз подій інформаційної безпеки в рамках їх життєвого циклу (наприклад, для

корпоративних інформаційних систем)» на підставі аналізу подій ІБ дає змогу мінімізувати потенційні ризики, пов'язані з можливими втратами інформаційних ресурсів корпорації, отже, мінімізує потенційну економічну шкоду за умови недотримання політики інформаційної безпеки корпорації.

Висновки. За підсумками аналізу світової практики управління корпоративною інформаційною безпекою запропоновано алгоритм реалізації адаптивного процесу Управління подіями інформаційної безпеки корпорацій. На відміну від наявних рішень, цей алгоритм має підпроцес «Обробка подій», який дає змогу здійснювати комплексну деталізацію процесу управління подіями інформаційної безпеки корпорацій та врахувати їх життєвий цикл. Проведені дослідження дають змогу на практиці заповнити потенційні прогалини інформації за створення СУІБ корпорацій. Додатковою перевагою запропонованого рішення є можливість задіяння цього підпроцесу як незалежного, що спрощує процедуру управління інформаційною безпекою корпорації загалом та сприяє зниженню витрати на її побудову.

З огляду на необхідність визначення економічної ефективності політики управління ІБ компанії, у подальших дослідженнях доцільно детальніше зупинитися на алгоритмізації підпроцесу «Обробка та аналіз подій ІБ в рамках їх життєвого циклу». Саме цей підпроцес дасть змогу здійснювати постійний моніторинг досягнення цілей і завдань функціонування системи інформаційної безпеки та визначення напрямів необхідних змін.

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. White, G. (2021). Generation Z: Cyber-Attack Awareness Training Effectiveness. *Journal of Computer Information Systems*, 1-12.
2. Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248.].
3. Хох В. Д., Мелешко Є. В., Смірнов О. А. Дослідження методів аудиту систем управління інформаційною безпекою. *Системи управління, навігації та зв'язку. Збірник наукових праць*, 2017. Вип. *1*(41). С. 38-42.
4. Shatnawi, M. M. (2019). Applying Information Security Risk Management Standards Process for Automated Vehicles. Bánki Közlemények (Bánki Reports), 2(1), 70-74.
5. Gabriel, R., Hoppe, T., Pastwa, A., & Sowa, S. (2009). Analyzing malware log data to support security information and event management: Some research results. In 2009 First International Confernce on Advances in Databases, Knowledge, and Data Applications (pp. 108-113). IEEE.
6. Bhatt, S., Manadhata, P. K., & Zomlot, L. (2014). The operational role of security information and event management systems. IEEE security & Privacy, 12(5), 35-41.
7. Kang, K., & Kim, J. (2015). A case study on converged security with event correlation of physical and information security. International Journal of Security and Its Applications, 9(9), 77-94.

8. Lopez, M. A., Silva, R. S., Alvarenga, I. D., Rebello, G. A., Sanz, I. J., Lobato, A. G., & Pujolle, G. (2017, October). Collecting and characterizing a real broadband access network traffic dataset. In 2017 1st Cyber Security in Networking Conference (CSNet) (pp. 1-8). IEEE.
9. Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. Information & management, 46(5), 267-270.
10. Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: factors of success. Entrepreneurship and Sustainability Issues, 6(4), 2081.
11. Shatnawi, M. M. (2019). Applying Information Security Risk Management Standards Process for Automated Vehicles. Bánki Közlemények (Bánki Reports), 2(1), 70-74.
12. Renners, L., Heine, F., & Rodosek, G. D. (2017, September). Modeling and learning incident prioritization. In 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (Vol. 1, pp. 398-403). IEEE.
13. Tanadi, Y., Soeprajitno, R. R. W. N., Firmansah, G. L., & El Karima, T. (2021). ISO 27001 Information Security Management System: Effect of Firm Audits in Emerging Blockchain Technology. *Riset Akuntansi dan Keuangan Indonesia*, *6*(2), 198-204.
14. Wu, W., Shi, K., Wu, C. H., & Liu, J. (2021). Research on the Impact of Information Security Certification and Concealment on Financial Performance: Impact of ISO 27001 and Concealment on Performance. *Journal of Global Information Management (JGIM)*, *30*(3), 1-16.
15. Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: factors of success. Entrepreneurship and Sustainability Issues, 6(4), 2081
16. Ko, K., Kim, H. K., Kim, J., Lee, C. Y., Cha, S. G., & Jeong, H. C. (2009, August). Design and Implementation of SIP-aware Security Management System. In International Workshop on Information Security Applications (pp. 10-19). Springer, Berlin, Heidelberg.

REFERENCES

1. White, G. (2021). Generation Z: Cyber-Attack Awareness Training Effectiveness. *Journal of Computer Information Systems*, *1-12* [in English].
2. Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. [in English].
3. Hoh, V. D., Meleshko, Je. V., & Smirnov, O. A. (2017). Doslidzhennja metodiv audytu system upravlinnja informacijnoju bezpekoju [Study of auditing methods of information security management systems]. *Systemy upravlinnja, navigacii' ta zv'jazku. Zbirnyk naukovyh prac' – Control, navigation and communication systems. Collection of scientific works*, (issue 1(41), (pp. 38-42) [in Ukrainian].
4. Shatnawi, M. M. (2019). Applying Information Security Risk Management Standards Process for Automated Vehicles. Bánki Közlemények (Bánki Reports), 2(1), 70-74 [in English].
5. Gabriel, R., Hoppe, T., Pastwa, A., & Sowa, S. (2009). Analyzing malware log data to support security information and event management: Some research results. In 2009 First International Confernce on Advances in Databases, Knowledge, and Data Applications (pp. 108-113). IEEE [in English].
6. Bhatt, S., Manadhata, P. K., & Zomlot, L. (2014). The operational role of security information and event management systems. IEEE security & Privacy, 12(5), 35-4 [in English].

7. Kang, K., & Kim, J. (2015). A case study on converged security with event correlation of physical and information security. International Journal of Security and Its Applications, 9(9), 77-94 [in English].
8. Lopez, M. A., Silva, R. S., Alvarenga, I. D., Rebello, G. A., Sanz, I. J., Lobato, A. G., & Pujolle, G. (2017, October). Collecting and characterizing a real broadband access network traffic dataset. In 2017 1st Cyber Security in Networking Conference (CSNet) (pp. 1-8). IEEE [in English].
9. Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. Information & management, 46(5), 267-270.
10. Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: factors of success. Entrepreneurship and Sustainability Issues, 6(4), 2081[in English].
11. Shatnawi, M. M. (2019). Applying Information Security Risk Management Standards Process for Automated Vehicles. Bánki Közlemények (Bánki Reports), 2(1), 70-74 [in English].
12. Renners, L., Heine, F., & Rodosek, G. D. (2017, September). Modeling and learning incident prioritization. In 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (Vol. 1, pp. 398-403). IEEE [in English].
13. Tanadi, Y., Soeprajitno, R. R. W. N., Firmansah, G. L., & El Karima, T. (2021). ISO 27001 Information Security Management System: Effect of Firm Audits in Emerging Blockchain Technology. *Riset Akuntansi dan Keuangan Indonesia*, *6*(2), 198-204 [in English].
14. Wu, W., Shi, K., Wu, C. H., & Liu, J. (2021). Research on the Impact of Information Security Certification and Concealment on Financial Performance: Impact of ISO 27001 and Concealment on Performance. *Journal of Global Information Management (JGIM)*, *30*(3), 1-16 [in English].
15. Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: factors of success. Entrepreneurship and Sustainability Issues, 6(4), 2081 [in English].
16. Ko, K., Kim, H. K., Kim, J., Lee, C. Y., Cha, S. G., & Jeong, H. C. (2009, August). Design and Implementation of SIP-aware Security Management System. In International Workshop on Information Security Applications (pp. 10-19). Springer, Berlin, Heidelberg. [in English].

Надійшла до редакції 31.10.2022.
Прийнято до друку 02.11.2022.
Публікація онлайн 23.12.2022.