DOI: https://doi.org/10.32782/2308-1988/2024-48-19
УДК 005.8

Горбаченко Станіслав Анатолійович
доктор економічних наук, професор, завідувач кафедри кібербезпеки,
Національний університет «Одеська юридична академія»

Stanislav Horbachenko
National University "Odesa Law Academy"

МІСЦЕ МЕНЕДЖМЕНТУ КІБЕРБЕЗПЕКИ У СУЧАСНІЙ УПРАВЛІНСЬКІЙ НАУЦІ ТА ПРАКТИЦІ

THE PLACE OF CYBERSECURITY MANAGEMENT IN MODERN MANAGEMENT SCIENCE AND PRACTICE

Анотація. Розглянуто теоретичні питання впливу кіберсередовища на сучасне управління та висловлено гіпотезу щодо необхідності адаптації наявних управлінських методик, технологій та інструментів для забезпечення максимальної ефективності та результативності менеджменту. Доведено важливість трансформації теорії та практики менеджменту у відповідності до процесів інформатизації та вимог кібербезпеки, які, у свою чергу, включають технічні, нормативно-правові, соціальні, економічні та інші аспекти. Обґрунтовано, що інтеграція менеджменту кібербезпеки в сучасну управлінську теорію та практику вимагає комплексного міждисциплінарного підходу. Висвітлено, як використовуються принципи менеджменту кібербезпеки на рівні операційних завдань, включаючи забезпечення захисту, цілісності та доступності інформації. Доведено, що менеджмент кібербезпеки виступає стратегічним елементом організаційної культури, розглядаючи питання безпеки в кіберсередовищі. Зроблено пропозиції щодо поетапного впровадження системи менеджменту кібербезпеки на рівні окремих підприємств та організацій.

Ключові слова: менеджмент, кіберсередовище, система; безпека, кіберзагроза, стратегія.

Summary. The article delves into the transformative aspects of "cybersecurity management" within theoretical research realms, aiming to seamlessly integrate various methods, measures, and tools into the management practices of domestic enterprises and organizations. It emphasizes the importance of cybersecurity management in today's technologically advanced and risk-laden landscape, proposing the application of methodologies like OCTAVE or ISO 27005. The practical implications of the study are significant. At the operational level, cybersecurity management is not just about safeguarding information but also ensuring its integrity and availability. This involves a combination of sophisticated technical solutions and the cultivation of a well-informed and trained workforce. The strategic dimension of cybersecurity management underscores the establishment of a robust organizational culture. This culture should prioritize security within the cyber environment, underlining its critical role in the overall health and safety of an organization. The article highlights the scientific novelty of the topic in the context of a rapidly evolving technological environment where risks and uncertainties are increasingly challenging to manage. It posits the need for developing new risk management strategies, which are adaptable to emerging threats and opportunities, and identifying effective decision-making criteria to handle these risks. From a practical standpoint, the significance of the article lies in its advocacy for the implementation of effective cybersecurity management practices in organizations. It supports endeavors to fortify security in the digital world, emphasizing the need for a comprehensive and interdisciplinary approach to cybersecurity management. This approach is vital given the multidimensional nature of cybersecurity, intertwining technical, human, and strategic elements. Furthermore, the article sheds light on the practical applications of cybersecurity management principles at the operational level, such as safeguarding the protection, integrity, and availability of information. It also illustrates how cybersecurity management evolves into a strategic cornerstone of organizational culture, addressing various security issues in the cyber environment. In summary, the article offers a thorough examination of cybersecurity management from both theoretical and practical perspectives. It proposes integrating specific methodologies into management practices, enhancing the operational and strategic facets of cybersecurity within organizations. The article underscores the necessity of developing new strategies and decision-making criteria in the face of ever-evolving technological risks and uncertainties, advocating for a holistic and interdisciplinary approach to managing cybersecurity. This comprehensive view is pivotal for fostering an organizational culture that prioritizes cybersecurity, ultimately contributing to the resilience and security of the digital infrastructure in modern enterprises and organizations.

Keywords: management, cyberspace, system, security, cyberattack, strategy.

© Горбаченко С. А., 2024

Постановка проблеми. Адаптація теорії та практики менеджменту до наслідків четвертої промислової революції, які виявляються у перетворенні автоматизованого виробництва, систем обміну даних і виробничих технологій на єдину саморегульовану систему, з мінімальним втручанням людини у виробничий процес або взагалі без нього, проходить досить складно. Тим більше, що в межах сучасної теорії та практики менеджменту інформаційні технології розглядаються не тільки в якості інструменту для підвищення ефективності діяльності підприємств та організацій, окремих галузей або національної економіки в цілому, а й як джерело кіберзагроз.

З іншого боку і проблеми кібербезпеки почали досліджуватися не лише в контексті технічного захисту. Адже тенденції останніх років свідчать про посилення людського чиннику при здійсненні кібератак, особливо в умовах розповсюдження аутсорсінгу, віддаленої роботи та активізації використання хмарних технологій. Тому обізнаність щодо питань інформаційної та кібербезпеки, а також створення відповідної культури в межах підприємства чи організації, набувають статусу повноцінного елементу кіберзахисту. Відтак до процесів пов'язаних з кібербезпекою більш активно починає залучатися саме управлінський персонал, а менеджмент кібербезпеки перетворюється на важливий елемент управлінської теорії та практики.

Аналіз останніх досліджень і публікацій. Оскільки кібербезпека виступає критично важливим аспектом для успішної діяльності будь-якого підприємства чи організацій у цифровому світі, вона поступово перетворюється й на важливий напрям міждисциплінарних досліджень і фігурує у наукових працях таких авторів як І. Діордіца, О. Довгань, І. Доронін, К. Краус, Н. Краус, О. Штепа та багатьох інших. У свою чергу управлінську складову кібербезпеки досліджували А. Штангрет, Я. Котляревський, М. Караїм, В. Панченко. Однак, у межах вищевказаних досліджень досі не сформовано єдиної концепції менеджменту кібербезпеки.

Мета та завдання статті. Головною метою статті є трансформація категорії «менеджмент кібербезпеки» в межах теоретичних досліджень, а також формування пропозицій щодо інтеграції окремих методів, заходів та інструментів менеджменту кібербезпеки в управлінську практику вітчизняних підприємств та організацій.

Актуальність дослідження. Швидка еволюція технологій вимагає переосмислення традиційних підходів до управління. Вирішення поточних управлінських завдань підвищеної складності за умов «мінімального втручання людини» потребує не тільки покращення матеріально-технічної бази, а й вивчення нових моделей організаційної структури та управління персоналом. Забезпечення захисту інформації в умовах зростаючих кіберзагроз вимагає від підприємств та організацій створення певної культури, яка знаходить своє відображення в менеджменті кібербезпеки.

Виклад основного матеріалу дослідження. Питання безпеки в менеджменті розглядаються як важлива складова успішного функціонування будь-якого підприємства чи організації. Адже наявність належного рівня безпеки сприятливо впливає на імідж, викликає довіру у контрагентів, клієнтів та органів державної та місцевої влади, зменшує вірогідність фінансових втрат, мотивує персонал тощо. У свою чергу загрози безпеці виступають як певні чинники, що формують небезпеку, тобто наявну та об'єктивну ймовірність негативного впливу на систему.

З огляду на це під менеджментом безпеки найчастіше розуміють систематизовані й скоординовані види діяльності, методи та засоби, за допомогою яких організація оптимально управляє своїми ризиками і пов'язаними з ними потенційними загрозами і впливами [1, с. 67].

Менеджмент безпеки здійснюється за принципами локалізації людського фактору, розуміння критичних місць та джерел небезпеки, моніторингу ризиків, можливості оперативного реагування. Щодо конкретних інструментів, які використовує менеджмент безпеки, можна зазначити наступні:

– оцінка фізичних, технічних та інформаційних ризиків, а також загроз з боку зовнішніх факторів;

– розробка політик безпеки, які включаються до загальної стратегії організації і повинні визначати стандарти та вимоги безпеки, правила поведінки працівників та процедури реагування на надзвичайні ситуації;

– навчання працівників з питань безпеки, встановлення систем безпеки та контролю, захист інформації, фізична охорона та інші відповідні заходи;

– встановлення та сприяння виконанню національних та міжнародних стандартів безпеки, наприклад, з охорони праці, безпеки продукції, інформаційної безпеки тощо;

– періодичний аудит та оцінка системи безпеки з метою виявлення слабких місць та вдосконалення існуючих процесів.

Враховуючи сучасні інформаційні перетворення, основним джерелом небезпеки для будь-якого підприємства чи організації все частіше стає кіберсередовище. Так, у 2022 році на прохання назвати свої найбільші побоювання, 44% керівників підприємств та організацій вказали на інциденти з кібербезпекою, і це набагато більше, ніж тих, хто назвав пандемію (22%) або рецесію (11%) [2]. Тому майже всі великі корпорації прагнуть оновити власну політику безпеки і роз-

робити методи ефективного реагування якраз з урахуванням кіберзагроз. Однак переважна більшість представників малого та середнього бізнесу все ще не до кінця усвідомлюють рівень вказаних загроз та масштаби можливих втрат (далеко не всі з яких можна виміряти кількісно).

Під кіберзагрозою розуміють протиправні, карані дії суб'єктів інформаційних правовідносин, які створюють небезпеку життєво важливим інтересам людини, суспільства та держави в цілому, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, а також відносинам щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації [3, с. 102].

Щодо конкретних прикладів кіберзагроз, можна навести промислове шпигунство, купівлю-продаж піратських програмних продуктів, несанкціоноване втручання в бази даних, недобросовісне використання інформації працівниками тощо [4]. Але найбільшу небезпеку для підприємств та організацій, безумовно, спричиняють кібератаки, об'єктами яких можуть бути майже усі складові підприємницької діяльності: фінанси, логістика, бренд, клієнти та їх персональні дані, фінанси тощо. Підґрунтям для ефективності кібератак є те, що суб'єкти підприємництва не завжди використовують надійне антивірусне ПЗ чи спеціалізовані рішення щодо захисту від DDoS-атак, вживають дій для захисту інформації та фінансових транзакцій, проводять відповідні тренінги для персоналу усіх ланок.

З іншого боку й спектр сучасних кібератак також є досить різнорідним, тож доцільно їх класифікувати за такими базовими ознаками, як: інструментальний засіб, що використовується при проведенні; специфіка реалізації; міра складності; умова ініціалізації; дистанційність; процес автоматизації; зовнішній прояв; спрямованість кінцевого результату та специфіка порушення базових характеристик системи інформаційної безпеки [5].

Найбільш масштабні кібератаки здійснюються на об'єкти критичної інфраструктури, тобто підприємства та установи, які є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, а виведення з ладу або руйнування їх може вплинути на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків та, навіть, людських жертв. Об'єкти критичної інфраструктури зосереджені, насамперед, в таких сферах, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації, продовольство, охорона здоров'я, комунальне господарство тощо.

Якщо мова йде про суб'єктів малого та середнього бізнесу, розповсюдженим інструментом для кібератак виступає також фішинг, тобто незаконне отримання конфіденційних даних користувачів обманним шляхом, наприклад за допомогою шахрайських повідомлень через соціальні мережі з використанням різних типів вірусних програм. Кіберзлочинці змушують користувачів передавати паролі, номери соціального страхування, отримують доступ до номерів платіжно-розрахункових карт і PINкодів, адресних книг, історій відвідувань і закладок у браузері тощо [6, с. 184].

Відповідно, підприємства та організації (насамперед ті, що відносяться до критичної інфраструктури), які зазнавали невпинних атак, розуміють, що можуть захистити свої дані, лише інвестуючи в комплексну систему управління кібербезпекою. Слід зауважити, що існує певна відмінність між термінами «система управління кібербезпекою» та «кібербезпека». Адже управління кібербезпекою зосереджується на способах організації активів, людей та процесів безпеки, в той час як кібербезпека виступає як загальна назва для захисту цифрової інфраструктури організації.

Якщо конкретизувати основні завдання підприємств при побудові системи управління кібербезпекою, ними виступають виявлення потенційних загроз і вразливостей, попередження кіберінцидентів, а також нейтралізація або мінімізація загроз інформаційної безпеки підприємства [7].

З огляду на вищевказане у менеджменті безпеки поступово формується окремий самостійний напрям – менеджмент кібербезпеки. Під останнім слід розуміти систему методів, заходів, інструментів спрямованих на мінімізацію ризиків та оптимізацію діяльності підприємства чи організації в кіберпросторі.

Як управлінська практика менеджмент кібербезпеки передбачає, насамперед інтеграцію в ІТ середовище таких принципів управління як цілеспрямованість, спланованість, компетентність, дисципліна, стимулювання, ієрархічність (рис. 1).

Принцип цілеспрямованості передбачає чітку постановку цілей щодо забезпечення кібербезпеки в межах власної зони впливу перед кожним структурним елементом підприємства та організації, а також визначення співвідношення цих цілей з необхідними для їхнього досягнення ресурсами. При цьому, якщо мова йде про фінансові ресурси, вартість розробки, впровадження та підтримки системи менеджменту кібербезпеки може значно варіюватися в залежності від таких чинників як розмір і складність організації, обсяг даних, які необхідно захистити, рівень ризику, бажаний рівень захисту тощо. Також в процесі розрахунку бюджету системи менеджменту кібербезпеки треба враховувати, що вказана система потребує не тільки разових стартових витрат на впровадження, а й поточних – на оцінку, оновлення, модернізацію тощо.

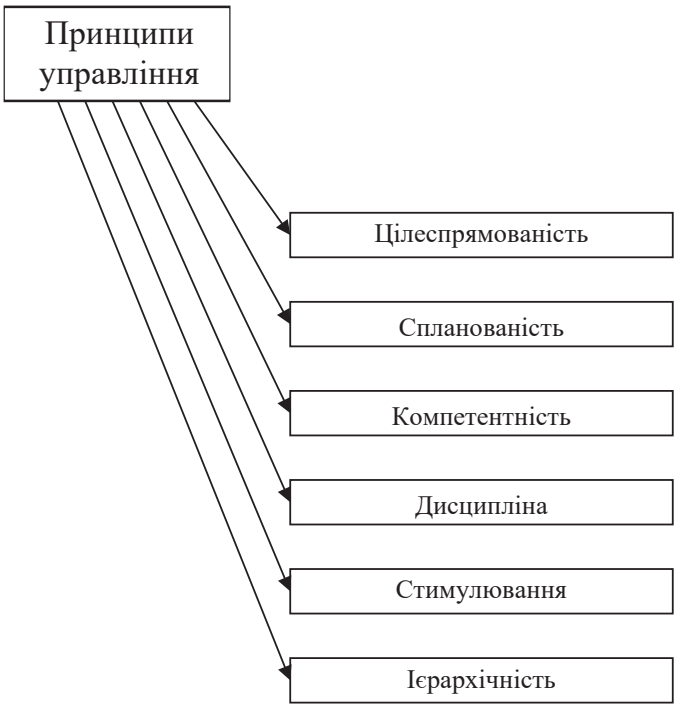

Рисунок 1 – Принципи менеджменту кібербезпеки

Джерело: сформовано автором

Принцип спланованості припускає складання на рівні менеджменту певної програми дій щодо кібербезпеки та захисту інформації, а також забезпечення її подальшої реалізації. Адже ефективне планування сприяє здійсненню координації дій виконавців (що є надважливим, адже питаннями кібербезпеки мають опікуватися представники всіх підрозділів підприємства чи організації), а також обліку і контролю за виконанням кожного окремого заходу і програми в цілому. В цьому сенсі менеджмент кібербезпеки обов'язково повинен бути органічно вбудований у процеси стратегічного планування.

Принцип компетентності ґрунтується на горизонтальному поділі праці і означає знання менеджером об'єкта управління, а також його особисті професійні навички та вміння налагодити комунікації із фахівцями у окремих питаннях. Підготовка менеджерів з кібербезпеки має враховувати такі її аспекти, як: мережева кібербезпека (захист комп'ютерів від зловмисників, шкідливих програм; безпека додатків (захист програмного забезпечення і пристроїв від кіберзагроз); інформаційна безпека (захист цілісності і конфіденційності даних під час їх зберігання чи передачі); аварійна безпека і безперервність бізнесу (реагування на аварійні ситуації в області кібербезпеки, які призводять до втрати операцій або даних); операційна безпека (забезпечення обробки і захист даних) [8].

На рівні вищого керівництва заслуговує уваги практика призначення великими корпораціями спеціального члена правління, а саме, директора з інформаційної безпеки (CISO) для нагляду за стратегією управління кібербезпекою. Серед його основних завдань можна відзначити нагляд за первинною архітектурою безпеки, а також оцінка будь-яких нових послуг на предмет потенційної вразливості; керівництво рішеннями щодо змін в IT-інфраструктурі; організація навчання користувачів найкращим практикам кіберзахисту тощо. Крім того, CISO повинен займатися організаційними питаннями, подібно до інших виконавчих лідерів. Це означає збалансування бюджету департаменту та роботу з іншими керівниками над розробкою бізнес-стратегії.

Принцип дисципліни розуміє під собою безумовне виконання вказівок керівника, посадових обов'язків, директив, інструкцій, наказів. Саме рівень дисципліни значною мірою визначає те, як підприємства та організації використовують наявні засоби безпеки, включаючи програмне забезпечення та рішення з IT-безпеки.

Принцип стимулювання передбачає зацікавленість всіх співробітників в дотриманні норм кібербезпеки на основі використання певної сукупності матеріальних і моральних стимулів. Можна зазначити, що менеджмент кібербезпеки використовує, переважно, моральне стимулювання яке виявляється у психологічному впливі на працівників та роз'ясненні важливості захисту інформації і обережності при роботі в кіберсередовищі.

Принцип ієрархічності має ґрунтуватися на вертикальному поділі управлінської праці, тобто

Таблиця 1 – Етапи впровадження системи менеджменту кібербезпеки

Назва етапу	Характеристика етапу
Оцінка ризиків кібербезпеки	Аналіз потенційних загроз за допомогою, наприклад, методології OCTAVE або методики ISO 27005.
Розробка політики кібербезпеки	Створення документу, який містить вимоги щодо забезпечення кібербезпеки на підприємстві чи в організації. У цьому документі можуть бути визначені правила використання інформаційних ресурсів, ролі та відповідальні за безпеку, правила зберігання та обробки інформації, процедури реагування на кібератаки тощо.
Вибір заходів забезпечення кібербезпеки	Обираються конкретні заходи, спрямовані на забезпечення кібербезпеки. Вони можуть бути технічні (наприклад, встановлення брандмауера, антивірусного програмного забезпечення тощо), чи організаційні (наприклад, проведення навчань з кібербезпеки для співробітників підприємства).
Розробка процедур кібербезпеки	Розробляються процедури, які описують алгоритм дій у випадку кібератаки або інших подій, що стосуються кібербезпеки.
Впровадження та підтримка системи менеджменту кібербезпеки	Впровадження всіх розроблених заходів, зокрема, проведення регулярних оглядів безпеки, оновлення технологій та політик, підтримку навчальних програм та інше.

Джерело: сформовано автором

виділенні рівнів управління і підпорядкування нижчих рівнів управління вищим. Зокрема, керівництво на вищому рівні повинне визначити стратегічні цілі забезпечення кібербезпеки, а також алокацію ресурсів та інвестицій у цей напрямок. В той самий час як менеджмент середньої ланки має забезпечити ефективне планування, реалізації та контроль за виконанням окремих заходів з кібербезпеки.

Формування системи менеджменту кібербезпеки в межах окремого підприємства чи організації складається з певної послідовності етапів (табл. 1).

Слід зауважити, що підприємства та організації можуть самостійно побудувати власну систему менеджменту кібербезпеки або звернутися до зовнішніх консультантів, які також можуть проаналізувати ситуацію та розробити стратегію захисту на випадок різних інцидентів.

Головне, щоб вище керівництво визнало наявність кіберризиків і взяло на себе лідерство та відповідальність в процесі впровадження менеджменту кібербезпеки. При цьому заходи кібербезпеки необхідно вживати не тільки для самого підприємства чи організації, але й для всього ланцюга постачання, включаючи бізнес-партнерів та аутсорсингові компанії.

В цьому сенсі, задля збільшення взаємної довіри, потрібно належним чином комунікувати з усіма зацікавленими сторонами, наприклад, шляхом надання інформації про можливі ризики та відповідні заходи з кібербезпеки у штатних та надзвичайних ситуаціях. Тобто, менеджмент кібербезпеки повинен бути інтегрований у всі процеси та рівні управління підприємством чи організацією, враховувати нові тенденції та загрози в сфері кібербезпеки, а також підтримувати планові зміни та вдосконалення.

Висновки. Управлінські методики, технології та інструменти майже неможливо перенести з одного середовища в інше без відповідної адаптації зі збереженням належного рівня ефективності та результативності. Тому процеси, які відбуваються і, навіть, формують кіберсередовище потребують відповідної трансформації теорії та практики менеджменту. Відтак, як об'єкт для подальших наукових досліджень менеджмент кібербезпеки виступає як комплексна міждисциплінарна проблема, яка має технічної, нормативно-правову, соціальну, економічну та інші складові.

В той самий час у практичному використанні на рівні операційних завдань менеджмент кібербезпеки має вирішувати питання щодо забезпечення не тільки захисту, а й цілісності та доступності інформації за допомогою як технічних рішень, так і відповідної роз'яснювальної та навчальної роботи з персоналом. А в стратегічному значенні менеджмент кібербезпеки повинен стати фундаментом відповідної організаційної культури, в центрі якої знаходяться саме питання безпеки в кіберсередовищі.

Список використаних джерел:

1. Штангрет А.М., Котляревський Я.В., Караїм М.М. Економічна безпека підприємства в умовах антикризового управління: концептуальне визначення та механізм забезпечення : монографія. Львів : Укр. акад. друкарства, 2012. 288 с.

2. Барометр ризиків Allianz. 2022. URL: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

3. Діордіца І. Поняття і зміст кіберзагроз на сучасному етапі. *Адміністративне право і процес.* 2017. № 4. С. 99–107.

4. Панченко В.А. Менеджмент інформаційної безпеки комерційного підприємства. URL: http://economics.kntu.kr.ua/pdf/3(36)/23.pdf

5. Довгань О.Д., Доронін І. М. Ескалація кіберзагроз національним інтересам України та правові аспекти кібербезпеки : монографія. Київ : Видавничий дім «АртЕк», 2017. 107 с.

6. Половенко Л., Мерінова С. Виявлення ознак соціальної інженерії та технологія протидії соціальним хакерам на підприємстві. *Підприємництво та інновації*. 2019. № 10. С. 183–187.

7. Краус К.М., Краус Н.М., Штепа О.В. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. 2022. URL: https://elibrary.kubg.edu.ua/id/eprint/42325/1/Kraus_Tsyfrova_transformatsiia_kiberbezpeky_2022.pdf

8. Євсюкова О.В. Особливості підготовки фахівців у сфері кібербезпеки: сучасні виклики та перспективи. 2021. URL: http://www.dy.nayka.com.ua/pdf/2_2021/4.pdf

References:

1. Stangret A. (2012) *Ekonomichna bezpeka pidpryiemstva v umovakh antykryzovoho upravlinnia: kontseptualne vyznachennia ta mekhanizm zabezpechennia* [Economic Security of an Enterprise in the Context of Crisis Management: Conceptual Definition and Mechanism of Ensuring]: monograph. Lviv: Ukrainian Academy of Printing, 288 p. (in Ukrainian)

2. Barometr ryzykiv Allianz [The Allianz risk barometer]. Available at: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html (in Ukrainian)

3. Diorditsa I. (2017) Poniattia i zmist kiberzahroz na suchasnomu etapi [The Concept and Content of Cyber Threats at the Present Stage]. *Administrative law and process*, no. 4, pp. 99–107. (in Ukrainian)

4. Panchenko V. Menedzhment informatsiinoi bezpeky komertsiinoho pidpryiemstva [Information security management of a commercial enterprise]. DOI: https://doi.org/10.32515/2663-1636.2019.3(36).219-228 (in Ukrainian)

5. Dovhan O., Doronin I. (2017) *Eskalatsiia kiberzahroz natsionalnym interesam Ukrainy ta pravovi aspekty kiberzakhystu* [Escalation of cyber threats to Ukraine's national interests and legal aspects of cyber defence]: monograph. Kyiv: ArtEk Publishing House, 107 p. (in Ukrainian)

6. Polovenko L., Merinova S. (2019) Vyiavlennia oznak sotsialnoi inzhenerii ta tekhnolohiia protydii sotsialnym khakeram na pidpryiemstvi [Identification of signs of social engineering and technology for counteracting social hackers at the enterprise]. *Підприємництво та інновації*, no. 10, pp. 183–187. (in Ukrainian)

7. Kraus K., Kraus N., Shtepa O. (2022) Tsyfrova transformatsiia kiberbezpeky na mikrorivni v umovakh voiennoho stanu [Digital transformation of cybersecurity at the micro level under martial law]. Available at: http://www.dy.nayka.com.ua/pdf/2_2021/4.pdf (in Ukrainian)

8. Yevsiukova O. (2021) Osoblyvosti pidhotovky fakhivtsiv u sferi kiberbezpeky: suchasni vyklyky ta perspektyvy [Peculiarities of training specialists in the field of cybersecurity: current challenges and prospects]. Available at: http://www.dy.nayka.com.ua/pdf/2_2021/4.pdf (in Ukrainian)

Стаття надійшла до редакції 11.01.2024