УДК 35.07:004.056](477)
DOI: https://doi.org/10.31470/2786-6246-2024-8-28-35

Вовк Артем,
аспірант Інституту держави і права імені В.М. Корецького НАН України

Vovk Artem,
graduate student of the V.M. Koretsky Institute of State and Law of National Academy of Sciences of Ukraine

ORCID ID: https://orcid.org/0009-0000-1294-3725

СУЧАСНІ ПРОБЛЕМИ ПУБЛІЧНОГО УПРАВЛІННЯ ЗАБЕЗПЕЧЕННЯМ КІБЕРБЕЗПЕКИ В УКРАЇНІ

CURRENT PROBLEMS OF PUBLIC ADMINISTRATION PROVIDING CYBER SECURITY IN UKRAINE

Анотація. У статті систематизовані наукові дослідження сучасних проблем публічного управління забезпеченням кібербезпеки в Україні.

Зазначено, що кібербезпека – це захист підключених до Інтернету систем, таких як обладнання, програмне забезпечення та бази даних від кіберзагроз. Ця практика використовується окремими особами, підприємствами та державою для запобігання несанкціонованому доступу до центрів обробки даних та інших комп'ютеризованих систем.

Звернуто увагу, що загрози постійно розвиваються, і ландшафт кібербезпеки постійно змінюється. Ставки у банківській та фінансовій індустрії високі, оскільки в небезпеці знаходяться значні грошові суми, а також існує ймовірність серйозних економічних потрясінь, якщо банки та інші фінансові системи будуть скомпрометовані. Теж саме стосується витоку персональних даних з органів державної влади та місцевого самоврядування.

Аналізуючи інноваційні підходи до кібербезпеки, виокремлені наступні методи: розвідка загроз, машинне навчання, поведінкова аналітика, архітектура нульової довіри, управління ризиками.

Виокремлені основні напрями вдосконалення публічного управління забезпеченням кібербезпеки в Україні: використання сучасних захисних технологій, обладнання комплексів, що дозволяють підняти її на найвищий рівень захищеності; підвищення кадрового потенціалу фахівців, здатних вирішувати складні технічні завдання щодо запобігання, обмеження та усунення сучасних кіберзагроз, їх умінь та професіоналізму; скоординовану діяльність суб'єктів кібербезпеки щодо попередження, виявлення та розкриття кіберзлочинів, комп'ютерних атак та кібертероризму; випереджаюче законодавче регулювання, відомчу нормативну правову регламентацію інституту кібербезпеки, протидію кіберзлочинності та кібертероризму, ліквідацію правових прогалин у максимально короткі терміни, відповідно до потреб правозастосовчої практики в цій сфері; активне використання сучасних форм, засобів та методів оперативно-розшукової діяльності, оперативно-розшукових заходів щодо забезпечення вищого рівня кібербезпеки та протидії кіберзлочинності; використання досвіду розвинених зарубіжних країн щодо організації кібербезпеки, протидії кіберзагрозам, боротьби з кібертероризмом та кримінальними кіберситуаціями; тиражування та впровадження у практичну діяльність досвіду забезпечення кібербезпеки, накопиченого різними міжнародними організаціями; створення, розвиток та вдосконалення організаційної та інформаційно-аналітичної служби у суб'єктах кібербезпеки; організація всебічних комплексних наукових досліджень проблем кібербезпеки, кіберзлочинності, кібератак та кібертероризму.

Ключові слова: публічне управління, органи державної влади, органи місцевого самоврядування, кібербезпека, кіберризики, кіберінциденти, інноваційні підходи до кібербезпеки, управління кіберризиками.

Abstract. The article systematizes scientific studies of modern problems of public management of cyber security in Ukraine.

The author states that cybersecurity is the protection of Internet-connected systems such as hardware, software, and databases from cyber threats. This practice is used by individuals, businesses, and the government to prevent unauthorized access to data centers and other computerized systems.

The author draws attention to the fact that threats are constantly evolving, and the landscape of cyber security is constantly changing. The stakes in the banking and financial industry are high, as large sums of money are at stake, and there is the potential for major economic upheaval if banks and other financial systems are compromised. The same applies to the leakage of personal data from state authorities and local governments.

The article highlights the following innovative approaches to cyber security: threat intelligence, machine learning, behavioral analytics, zero trust architecture, risk management.

The main areas of improvement of public management of cyber security in Ukraine are highlighted: the use of modern protective technologies, equipment and complexes, which allow to raise it to the highest level of security; increasing the personnel potential of specialists capable of solving complex technical tasks related to the prevention, limitation and elimination of modern cyber threats, their skills and professionalism; coordinated activity of cyber security entities regarding the prevention, detection and disclosure of cybercrime, computer attacks and cyber terrorism; anticipatory legislative regulation, departmental regulatory legal regulation of the cyber security institute, combating cybercrime and cyberterrorism, elimination of legal gaps in the shortest possible time, in accordance with the needs of law enforcement practice in this area; active use of modern forms, means and methods of operational and investigative activity, operational and investigative measures to ensure the highest level of cyber security and countering cybercrime; using the experience of developed foreign countries in the organization of cyber security, combating cyber threats, combating cyber terrorism and criminal cyber situations; replication and implementation in practical activities of the experience of ensuring cyber security accumulated by various international organizations; creation, development and improvement of organizational and information-analytical service in cyber security subjects; organization of comprehensive scientific research on the problems of cyber security, cybercrime, cyber-attacks and cyber terrorism.

Keywords: public administration, state authorities, local self-government bodies, cyber security, cyber risks, cyber incidents, innovative approaches to cyber security, cyber risk management.

Постановка проблеми. Кібербезпека є критичною проблемою в сучасну цифрову епоху, коли кіберзагрози стають все більш складними і витонченими. Для вирішення цих проблем потрібні інноваційні підходи до кібербезпеки. У цій статті розглядаються різні інноваційні стратегії та технології, які можуть бути використані для підвищення кібербезпеки. Ґрунтуючись на міждисциплінарних перспективах інформатики, інформаційних технологій, штучного інтелекту та поведінкової психології, в цьому дослідженні розглядаються нові тенденції та розробки в області кібербезпеки, включаючи аналіз загроз, машинне навчання, поведінковий аналіз, архітектуру з нульовою довірою, управління ризиками. Аналізуючи тематичні дослідження, передовий досвід галузі та нові технології, стаття покликана дати уявлення про те, як система органів влади може застосовувати інноваційні підходи для захисту своїх цифрових активів та ефективного зниження кіберризиків.

Кібербезпека – це захист підключених до Інтернету систем, таких як обладнання, програмне забезпечення та дані від кіберзагроз. Ця практика використовується окремими особами, підприємствами та державою для запобігання несанкціонованому доступу до центрів обробки даних та інших комп'ютеризованих систем.

Кібербезпека знаходить використання в різних областях, від бізнес-сфери до мобільних технологій. У цій течії можна виділити кілька особливо важливих категорій:

1. Безпека мереж – заходи та дії щодо захисту комп'ютерних мереж різного рівня загроз.
2. Безпека інформації – забезпечення цілісності та закритості даних під час зберігання, а також за її передачу.

Аналіз останніх досліджень і публікацій. Питання публічного управління забезпеченням кібербезпеки в Україні, основні інституційні та організаційні механізми публічного управління забезпеченням кібербезпеки, загрози та виклики сучасній кібербезпеці, правові аспекти публічного управління забезпеченням кібербезпеки, підготовка фахівців у даній галузі аналізують українські та закордонні вчені, у тому числі: Л. Арсенович, І. Артьомова, М. Бендас, К. Бонарєва, О. Бондаренко, С. Вдовенко, Ю. Даник, Л. Дешко, І. Доронін, І. Забара, В. Кравець, С. Мельник, Є. Нікітіна, О. Пермяков, Г. Піскорська, О. Потій, Г. Ситник, В. Шемчук, Н. Яковенко та ін.

Мета дослідження є систематизація наукових досліджень сучасних проблем публічного управління забезпеченням кібербезпеки в Україні.

Виклад основного матеріалу дослідження. Кібербезпека – це процес захисту від зловмисних вторгнень у мережі, комп'ютери, сервери, мобільні пристрої, електронні системи та дані. Її також називають безпекою інформаційних технологій або електронною інформаційною безпекою [1].

Кібербезпека має вирішальне значення, оскільки вона захищає від деяких з найсерйозніших проблем у галузі кібербезпеки, таких як крадіжка та знищення багатьох типів даних. Це включає конфіденційну інформацію, особисту інформацію, захищену медичну інформацію, персональні дані, дані про інтелектуальну власність та інформаційні системи, що використовуються урядом та підприємствами.

Небезпека кібербезпеки посилюється характеристиками мереж 5G. Споживачі, підприємства та міста по всій країні, які намагаються впровадити 5G, погано підготовлені для оцінки та усунення пов'язаних з ним небезпек. Як рішення вкрай важливо визначити особи сторонніх зловмисників, залучених у безперервний процес отримання незаконного доступу до даних користувачів та зловживання їхньою конфіденційністю та довірою до фірм або держави.

Зловмисники можуть запускати атаки на системи на основі блокчейну. Багато з цих атак використовували добре відомі методи, такі як фішинг, соціальна інженерія, атаки на дані при передачі та зосередження уваги на помилках кодування. Можна створити більш надійну технічну інфраструктуру за допомогою засобів контролю та стандартів кібербезпеки на основі блокчейну для захисту підприємств від кібератак. Також може знадобитися поєднання блокчейна з іншими передовими технологіями, такими як штучний інтелект, Інтернет речей та машинне навчання.

Недоліки програмного забезпечення, які можуть надати зловмиснику доступ до системи, відомі як вразливості в програмному забезпеченні. Ці недоліки можуть бути результатом помилки у кодуванні програмного забезпечення або у тому, як воно побудовано. Програмне забезпечення, що управляє вразливістю, має стратегію кібербезпеки. Воно запобіжно сканує мережу на наявність вразливостей, виявляє їх та пропонує рекомендації щодо усунення недоліків, щоб знизити ймовірність порушень безпеки в майбутньому.

ISSN 2786-6246 (print) ● ISSN 2786-9091 (online)

Загрози постійно розвиваються, і ландшафт кібербезпеки постійно змінюється. Ставки у банківській та фінансовій індустрії високі, оскільки в небезпеці знаходяться значні грошові суми, а також існує ймовірність серйозних економічних потрясінь, якщо банки та інші фінансові системи будуть скомпрометовані. Теж саме стосується витоку персональних даних з органів державної влади та місцевого самоврядування.

Транскордонний характер кіберпростору, який спільно використовується безліччю економічних агентів інформаційних та комунікаційних систем, створюють труднощі у вирішенні завдання попередження загроз кібербезпеці. Стратегії, що реалізуються державою, організаціями та окремими індивідами внаслідок їх тісного взаємозв'язку можуть мати суттєві наслідки для інших економічних агентів усередині країни та за її межами, а також впливати на стан цифрового простору. В даний час комп'ютерні атаки неухильно зростають як за кількістю, так і за складністю. Вони стають дедалі цілеспрямованішими і зачіпають не лише державу, а й приватний сектор. У цих умовах держава починає усвідомити стратегічну важливість даних та контролю над ними, а також необхідність створення надійної системи захисту від кіберризиків.

Повсюдне поширення цифрових технологій у всі сфери життєдіяльності сучасного суспільства роблять IT-компанії повноправними учасниками системи кібербезпеки держави. Це зумовлено тим, що створені ними інформаційні системи є об'єктом кібератак. І це змушує їх розробляти обладнання та програмне забезпечення, що використовуються для виявлення та захисту від кіберінцидентів. У зв'язку з цим співпраця між державним сектором та IT-компаніями стала необхідною умовою забезпечення кібербезпеки держави.

У червні 2022 р. Рада Всесвітнього економічного форуму з підключеного світу опублікувала звіт Global Action and Recent Progress Insight Report, в якому представлений короткий огляд помітних ініціатив у галузі управління технологіями у всьому світі. У звіті було виявлено деякі покращення щодо передового досвіду в галузі кібербезпеки, а також екологічних, соціальних та управлінських питань. Однак необхідна подальша робота, щоб справді забезпечити, щоб підключені пристрої приносили користь державам, компаніям, людям та планеті [2].

Повноваження щодо вдосконалення міжнародних стандартів кібербезпеки належать урядам, приватному сектору, органам стандартизації та іншим зацікавленим сторонам [3]. Усі сторони повинні скоординувати свої зусилля для заохочення впровадження передового досвіду, мінімізації транскордонних бар'єрів та зменшення фрагментації системи.

Міжнародна спільнота досягла значних успіхів у багатьох галузях управління технологіями, але, як і раніше, терміново необхідні додаткові дії, щоб максимізувати здатність технологій приносити користь суспільству. Це вимагає застосування системного підходу для аналізу витрат та вигод від технологічних інновацій та впровадження [4].

Основними суб'єктами кібербезпеки на даний час є посадові особи державних органів, органів місцевого самоврядування, наділених відповідними повноваженнями, серед яких особливо вирізняються: Міністерство цифрової трансформації України, Міністерство культури та інформаційної політики України, а також правоохоронні структури (Департамент кіберполіції Національної поліції України), Ситуаційний центр забезпечення кібербезпеки СБУ, а також інші органи державної влади, які забезпечують систему кібербезпеки в Україні.

Перелічені та інші суб'єкти кібербезпеки забезпечують її за допомогою правових, організаційних, технічних, оперативно-розшукових, кадрових, розвідувальних, контррозвідувальних, наукових, інформаційно-аналітичних заходів.

Аналізуючи інноваційні підходи до кібербезпеки, слід виокремити наступні методи: розвідка загроз, машинне навчання, поведінкова аналітика, архітектура нульової довіри, управління ризиками.

Одним із інноваційних підходів до кібербезпеки є використання розвідки загроз, яка включає збір, аналіз та поширення інформації про кіберзагрози та противників. Аналітика загроз дозволяє органам державної влади активно виявляти та знижувати кіберризики, розуміючи тактику, методи та процедури, що використовуються суб'єктами небезпек. Використовуючи дані про загрози, групи безпеки можуть виявляти загрози, що виникають, визначати пріоритетність заходів безпеки та ефективно реагувати на кіберінциденти. Платформи аналізу загроз об'єднують дані з різних джерел, включаючи дані з відкритих джерел, моніторинг даркнету та власні канали загроз, щоб надати дієву інформацію про кіберзагрози та тенденції їх розвитку.

Крім того, ініціативи щодо обміну інформацією про загрози сприяють співробітництву між організаціями, державними установами та галузевими партнерами, посилюючи колективний захист від кіберзагроз та підвищуючи загальну стійкість кібербезпеки.

Наступним інноваційним підходом до кібербезпеки є машинне навчання. Машинне навчання – це ще один інноваційний підхід до кібербезпеки, який використовує алгоритми штучного інтелекту для виявлення та пом'якшення кіберзагроз у режимі реального часу. Моделі машинного навчання аналізують величезні обсяги даних, включаючи мережевий трафік, поведінку користувачів та системні журнали, для виявлення закономірностей та аномалій, що вказують на шкідливу активність. Навчаючи алгоритми машинного навчання на історичних даних, системи кібербезпеки можуть навчитися розпізнавати відомі загрози та адаптуватися до методів атак, що розвиваються. Алгоритми контрольованого машинного навчання класифікують кіберзагрози на основі помічених даних, що вивчаються, а алгоритми неконтрольованого машинного навчання виявляють аномалії та викиди в наборах неструктурованих даних.

Крім того, методи глибокого навчання, такі як нейронні мережі, дозволяють системам кібербезпеки автоматично отримувати функції та закономірності з необроблених даних, підвищуючи точність виявлення та зменшуючи кількість хибних спрацьовувань.

Ще одним інноваційним підходом до кібербезпеки є поведінкова аналітика. Поведінкова аналітика – це передовий підхід до кібербезпеки, який фокусується на розумінні та прогнозуванні поведінки людини для виявлення та запобігання кіберзагроз. Платформи поведінкової аналітики аналізують активність користувачів, взаємодію пристроїв та поведінку системи, щоб виявити відхилення від нормальних шаблонів та виявити підозрілу поведінку, що вказує на внутрішні загрози, зламані облікові записи чи шкідливу діяльність. Встановлюючи базові профілі нормальної поведінки користувачів та об'єктів, системи поведінкової аналітики можуть виявляти аномалії, що вказують на потенційні інциденти безпеки. Крім того, поведінкова біометрія, така як динаміка натискання клавіш, руху миші та розпізнавання голосу, дозволяє організаціям аутентифікувати користувачів та виявляти спроби несанкціонованого доступу на основі унікальних поведінкових показників.

ISSN 2786-6246 (print) ● ISSN 2786-9091 (online)

Наступним інноваційним підходом до кібербезпеки є архітектура нульової довіри. Архітектура нульової довіри – це зсув парадигми в кібербезпеці, який передбачає відсутність довіри до користувачів, пристроїв або мереж та застосовує суворий контроль доступу та механізми автентифікації для перевірки та підтвердження кожної взаємодії. Архітектура нульової довіри використовує підхід до кібербезпеки «ніколи не довіряй, завжди перевіряй», вимагаючи безперервної автентифікації, авторизації та перевірки користувачів та пристроїв, які мають доступ до критично важливих ресурсів та даних. За рахунок реалізації мікросегментації, контролю доступу з мінімальними привілеями та протоколів шифрування архітектура нульової довіри зводить до мінімуму поверхню атаки, пом'якшує горизонтальне переміщення та запобігає несанкціонованому доступу до конфіденційної інформації. Крім того, архітектура з нульовою довірою інтегрується з рішеннями управління ідентифікацією та доступом (IAM), системами багатофакторної автентифікації (MFA) та платформами управління інформацією про безпеку та події (SIEM), щоб забезпечити комплексну видимість та контроль над цифровими активами та активністю користувачів.

Кібербезпека тісно пов'язана з оцінкою та управлінням ризиками – необхідною діяльністю для створення критичної інфраструктури та підтримки у прийнятті рішень. При плануванні відповідної інфраструктури кібербезпеки враховуються ширші завдання різних рівнів, включаючи підтримку економічного зростання, реалізацію організаційних цілей, навчання персоналу та ін. аналіз ризиків широко застосовується для прогнозування майбутніх подій [5; 6].

Стан системи кібербезпеки став одним з ключових індикаторів рівня розвитку країни поряд із класичними показниками (ВВП тощо). Отримало розвиток новий напрямок – «економіка кібербезпеки», що оцінює ризики та переваги для різних гравців (індивідів, організацій, держав) з точки зору потенційних кіберзагроз, їх поведінкові патерни, стратегії, а також вплив державного регулювання та ринкових механізмів на стан кібербезпеки [7].

Щодо національної безпеки превентивна оцінка ризиків допоможе мінімізувати загрози, вихідні з таких джерел, як міжнародні конфлікти, політичні протести, торгівля інсайдерською інформацією, атаки за допомогою шкідливих програм, шпигунство та ін. [8]. Для аналізу та усунення цих факторів використовуються різні методології управління ризиками.

Таким чином, інноваційні підходи до забезпечення кібербезпеки необхідні органам державної влади, організаціям, які прагнуть захистити свої цифрові активи та знизити кіберризики у сучасному середовищі загроз. Аналітика загроз, машинне навчання, поведінковий аналіз та архітектура нульової довіри являють собою передові технології та стратегії, які органи державної влади можуть використовувати для підвищення своєї кібербезпеки та захисту від кіберзагроз, що розвиваються. Прийнявши випереджальний та цілісний підхід до кібербезпеки, органи державної влади можуть покращити виявлення загроз, реагування на інциденти та загальну стійкість кібербезпеки, захищаючи свої дані, системи та мережі від кібератак.

Однак, ефективна кібербезпека потребує постійного моніторингу, адаптації та співпраці між зацікавленими сторонами, оскільки кіберзагрози розвиваються і поширюються на все більші взаємопов'язані та цифрові системи у світі. Завдяки впровадженню інноваційних підходів та передового досвіду в галузі кібербезпеки органи державної влади можуть знизити кіберризики, зміцнити довіру з боку зацікавлених сторін та забезпечити цілісність, конфіденційність та доступність своїх цифрових активів.

Висновки. Проведений аналіз дає підстави зазначити, що до основних напрямів вдосконалення публічного управління забезпеченням кібербезпеки в Україні та підвищення його ефективності можна віднести: використання сучасних захисних технологій, обладнання комплексів, що дозволяють підняти її на найвищий рівень захищеності; підвищення кадрового потенціалу фахівців, здатних вирішувати складні технічні завдання щодо запобігання, обмеження та усунення сучасних кіберзагроз, їх умінь та професіоналізму; скоординовану діяльність суб'єктів кібербезпеки щодо попередження, виявлення та розкриття кіберзлочинів, комп'ютерних атак та кібертероризму; випереджаюче законодавче регулювання, відомчу нормативно-правову регламентацію інституту кібербезпеки, протидію кіберзлочинності та кібертероризму, ліквідацію правових прогалин у максимально короткі терміни, відповідно до потреб правозастосовчої практики в цій сфері; активне використання сучасних форм, засобів та методів оперативно-розшукової діяльності, оперативно-розшукових заходів щодо забезпечення вищого рівня кібербезпеки та протидії кіберзлочинності; використання досвіду розвинених зарубіжних країн щодо організації кібербезпеки, протидії кіберзагрозам, боротьби з кібертероризмом та кримінальними кіберситуаціями; тиражування та впровадження у практичну діяльність світового досвіду забезпечення кібербезпеки, який накопичений у різних країнах; створення, розвиток та вдосконалення організаційної та інформаційно-аналітичної служби у суб'єктах кібербезпеки; організація всебічних комплексних наукових досліджень проблем кібербезпеки, кіберзлочинності, кібератак та кібертероризму.

Список використаних джерел:

1. Goodall, A. J. Cyber Security: Law and Practice. Sweet & Maxwell, 2020.
2. Future of the Connected World: Global Action and Recent Progress. URL: https://www3.weforum. org/docs/WEF_Future_of_the_Connected_World_2022.pdf (дата звернення: 23.03.2024).
3. AlDaajeh S., Saleous H., Alrabaee S., Barka E., Breitinger F., Choo K.K.R. The Role of National Cybersecurity Strategies on the Improvement of Cybersecurity Education. *Computers and Security*. 2022. № 119, 102754. https://doi.org/10.1016/j.cose.2022.102754.
4. Pollini A., Callari T.C., Tedeschi A., Ruscio D., Save L., Chiarugi F., Guerri D. Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach. *Cognition, Technology and Work*. 2022. № 24(2). P. 371–390. https://doi.org/10.1007/s10111-021-00683-y.
5. Michalec O., Milyaeva S., Rashid A. When the Future Meets the Past: Can Safety and Cyber Security Coexist in Modern Critical Infrastructures? *Big Data & Society.* 2022. № 9(1). 205395172211083. https://doi.org/10.1177/20539517221108369.
6. Rosado D.G., Santos-Olmo A., Sánchez L.E., Serrano M.A., Blanco C., Mouratidis H., Fernández-Medina E. Managing Cybersecurity Risks of Cyber-Physical Systems: The MARISMA-CPS Pattern. *Computers in Industry*. 2022. № 142. 103715. https://doi.org/10.1016/j. compind.2022.103715.
7. Jentzsch N. State-of-the-Art of the Economics of Cyber-Security and Privacy (IPACSO Deliverable D4.1), 2018. https://doi.org/10.2139/ ssrn.2671291.
8. McEvoy R., Kowalski S. Cassandra's Calling Card: Socio-Technical Risk Analysis and Management in Cyber Security Systems. In: CEUR Workshop Proceedings. 2019. Vol. 2398. P. 65–80.

References:

1. Goodall, A. J. (2020). *Cyber Security: Law and Practice*. Sweet & Maxwell [in English].
2. *Future of the Connected World: Global Action and Recent Progress.* Retrieved from https://www3.weforum.org/docs/WEF_Future_of_the_Connected_World_2022.pdf [in English].
3. AlDaajeh S., Saleous H., Alrabaee S., Barka E., Breitinger F., Choo K.K.R. (2022). The Role of National Cybersecurity Strategies on the Improvement of Cybersecurity Education. *Computers and Security, 119,* 102754. https://doi.org/10.1016/j.cose.2022.102754 [in English].

4. Pollini A., Callari T.C., Tedeschi A., Ruscio D., Save L., Chiarugi F., Guerri D. (2022). Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach. *Cognition, Technology and Work, 24(2),* 371–390. https://doi.org/10.1007/s10111-021-00683-y [in English].
5. Michalec O., Milyaeva S., Rashid A. (2022). When the Future Meets the Past: Can Safety and Cyber Security Coexist in Modern Critical Infrastructures? *Big Data & Society, 9(1),* 205395172211083. https://doi.org/10.1177/20539517221108369 [in English].
6. Rosado D.G., Santos-Olmo A., Sánchez L.E., Serrano M.A., Blanco C., Mouratidis H., Fernández-Medina E. (2022). Managing Cybersecurity Risks of Cyber-Physical Systems: The MARISMA-CPS Pattern. *Computers in Industry, 142,* 103715. https://doi.org/10.1016/j. compind.2022.103715 [in English].
7. Jentzsch N. (2018). *State-of-the-Art of the Economics of Cyber-Security and Privacy (IPACSO Deliverable D4.1).* https://doi.org/10.2139/ ssrn.2671291 [in English].
8. McEvoy R., Kowalski S. (2019). Cassandra's Calling Card: Socio-Technical Risk Analysis and Management in Cyber Security Systems. In: *CEUR Workshop Proceedings, 2398*, 65–80 [in English].

Подано до редакції 25.03.24 р.
Прийнято до друку 29.04.24 р.