DOI 10.34132/pard2025.27.12

Отримано: 30 серпня 2024
Змінено: 10 січня 2024
Прийнято: 3 лютого 2025
Опубліковано:
31 березня 2024

Received: 30 August 2024
Revised: 10 January 2024
Accepted: 3 February 2025
Published:
31 March 2025

Stanislav Larin

PROTECTION OF INFORMATION IN THE CYBERSECURITY SYSTEM AS A STRATEGIC IMPLEMENTATION PRIORITY FOR STATE MECHANISMS OF NATIONAL VALUES PROTECTION IN UKRAINE

The article analyses the research of information security threats in the cybersecurity system, which the author considers a strategic implementation priority for state mechanisms of national values protection in Ukraine.

The methodology of the study includes the method of ranking threats to information protection in the cybersecurity system, which is reflected through theoretical foundations and the method of expert research. The author focuses on contemporary methods of information protection in the cybersecurity system concerning the implementation of state mechanisms of national values protection in Ukraine. The results obtained by the researchers allowed us to identify a list of threats in the cybersecurity system to form an information basis for making and implementing management decisions.

The purpose of the article is to identify threats to information protection in the cybersecurity system as one of the strategic implementation priorities for state mechanisms of national values protection in Ukraine under martial law and prospects for transformational changes in public administration in the post-war period of Ukraine based on the theoretical and methodological analysis of scientific literature.

The results obtained by scientists in this area of activity have practical and scientific significance: due to the use of a methodological approach to the formation of information security requirements in the cybersecurity system, segments of strategic priorities for the protection of national values in Ukraine are considered. The author demonstrates the methods used to achieve this goal, in particular, the method of analysing the state of cybersecurity and the methods of description and classification, which contribute to the effective protection of information as one of the strategic implementation priorities for state mechanisms of national values protection in Ukraine.

The methodological approach specifies that it is advisable to describe and only then classify various types of threats and hazards, risks and challenges and, correspondingly, formulate a system of measures to manage them.

Common methods of analysing the level of cyber security assurance include methods of studying the cause-and-effect relationships between threats and hazards; the search for the reasons that caused and led to the actualisation of certain hazards is carried out. The author proposes measures to neutralise threats to information protection in the cybersecurity system as one of the strategic implementation priorities for state mechanisms of national values protection in Ukraine.

Key words: *state mechanisms of national values protection in Ukraine, strategic implementation priorities for state mechanisms, threats to information security, cybersecurity system, martial law, transformational changes in public administration.*

Постановка проблеми у загальному вигляді. В епоху технологічного домінування виникає постійна потреба в захисті інформації від хакерства. В нашій пам’яті постають нещодавні події, які пов’язані зі зламаним Київстар, який вибив з ладу мільйони користувачів, DDOS-атаки на Monobank із загальним навантаженням у 580 мільйонів запитів, які були успішно відбиті, та на сайти Міністерства юстиції України, Міністерства оборони України та ін., на яких було втрачено цінну державну інформацію.

Ці інциденти показали, що кібербезпека є актуальною та важливою сферою діяльності, і визначається як стратегічний пріоритет реалізації державних механізмів захисту національних цінностей в Україні. Адже, по суті, кібербезпека – це проактивний і реактивний підхід до захисту величезної кількості взаємопов'язаних пристроїв і систем, які є основою національної безпеки сучасної держави та її громадян. Це виходить за рамки простого захисту, щоб підкреслити постійну адаптацію та зміцнення нашої національної безпеки, представленої у вигляді цифрової інфраструктури, проти невпинної винахідливості кіберсупротивників.

Потреба в кібербезпеці вже давно виходить за межі особистого життя та сягає наших соціальних та економічних структур. Чим більше ми покладаємося на цифрові платформи для комунікацій, торгівлі та критичної інфраструктури, тим більшим є потенційний вплив кіберзагроз на особистість, організацію, державу. Адже йдеться не лише про захист апаратного та програмного забезпечення, а про захист нашого цифрового існування, зокрема: захист персональних даних особистості та організації; фінансовий захист; управління репутацією; збереження національної безпеки; безперервність ІТ-систем; захист енергетичних мереж тощо [1; 2].

Саме ці складові стали базовими із захисту інформації в системі кібербезпеки як стратегічного пріоритету реалізації державних механізмів захисту національних цінностей в Україні, що викликані світовими глобалізаційними процесами, і, зокрема, воєнним станом в Україні.

Аналіз останніх досліджень і публікацій. Більшість науковців зазначають, що у сучасному глобалізованому світі інформація та бази даних є тими унікальними ресурсами, без використання та збереження яких неможливе існування та розвиток як сучасної держави, так і соціально-політичного утворення, виконання суто військових завдань зі збереження незалежності і державності України [3; 4]. На думку вітчизняних та зарубіжних науковців та практиків Н. Чоудхурі, Е. Ністад, К. Регорд, В. Гкіулос [2], В. Ємельянова, У. Никоненко, Ю. Ситника, І. Охріменка, А. Шульги [3], сучасна агресія Росії в Україні визначається саме наявністю потужної інфор-

 DOI 10.34132/pard2025.27.12

маційно-кібернетичної складової. Доступ до інформації та захист процесів управління стають визначальними чинниками досягнення політичних цілей та перемоги ЗСУ.

Вітчизняні науковці М. Криштанович, В. Філіппова, М. Губа, О. Карташова, О. Молнар [4], П. Петровський, І. Хомишин, І. Безена, І. Сердечна [5], О. Гордєєв, В. Харченко, О. Ілляшенко, О. Морозова, М. Гасанов [6], А. Магрук [7], С. Криштанович, Н. Любомудрова, С. Тимофєєв, О. Шмигель, Г. Комісаренко [8] в своїх працях описують розвиток нових деструктивних практик у кіберпросторі, зокрема: кіберзлочинність, шпигунство в політичних чи економічних цілях, атаки на критичну інфраструктуру (транспорт, транспортні комунікації тощо) з диверсійною метою.

Автори зазначають, що ці кібератаки є: необмеженими кордонами чи відстанню; анонімними, і дуже важко дійсно ідентифікувати справжнього винуватця, часто діючи під виглядом ботнетів або посередників. Можна зробити висновок, що відносно легко ці кібератаки, з невеликими витратами або ризиком для зловмисника, спрямовані на те, щоб поставити під загрозу безперебійне функціонування інформаційних і комунікаційних систем, якими користуються громадяни, підприємства та органи управління, а також фізичну цілісність інфраструктури, що має вирішальне значення як для національної безпеки України, так і захисту її національних цінностей [9; 10].

Формулювання цілей статті (постановка завдання). Метою статті є методологічний аналіз наукової літератури щодо захисту інформації в системі кібербезпеки як одного зі стратегічних пріоритетів реалізації державних механізмів захисту національних цінностей в Україні, що викликані світовими глобалізаційними процесами.

Основним завданням є систематизація наукових підходів, що використовуються в контексті дослідження вченими світу із захисту інформації в системі кібербезпеки як одного зі стратегічних пріоритетів реалізації державних механізмів захисту національних цінностей в Україні, що викликані світовими глобалізаційними процесами, а також формулювання рекомендацій для мінімізації їх впливу на національну безпеку держави.

Виклад основного матеріалу дослідження. Важливим чинником розвитку сучасного суспільства є забезпечення захисту інформації та кібербезпеки, які визначаються ключовими елементами будь-яких процесів, незалежно від сфери суспільної діяльності. Особлива увага приділяється аналізу потенційних загроз захисту інформації в системі кібербезпеки як одного зі стратегічних пріоритетів реалізації державних механізмів захисту національних цінностей в Україні у сфері матеріальних, фінансових, репутаційних та інших втрат.

Для протидії загрозам кібербезпеки доцільно вжити заходи, які випливають із зниження вразливості об'єкта безпеки. Відповідно вітчизняними та зарубіжними науковцями та практиками були виокремлені два предметних напрямки протидії:

– сукупністю джерел загроз;
– сукупністю заходів забезпечення кібербезпеки.

Обидва напрямки протидії інформаційній та кібербезпеці охоплюють технічні, правові, організаційні, психологічні аспекти, зумовлюють надзвичайну складність та багаторівневість системних зв'язків між її складовими елементами [11].

У свою чергу, забезпечення кібербезпеки є безперервним процесом, який має системний характер і досягається впровадженням найбільш раціональних методів та комплексним використанням необхідних фізичних, апаратних, програмних, криптографічних засобів. Найкращий результат досягається тоді, коли всі використані засоби і методи об'єднані в єдиний державний механізм, функціонування якого необхідно відстежувати, оновлювати та доповнювати, залежно від змін як внутрішнього, так і зовнішнього середовища.

Окрім того, доцільно зазначити, що цей процес має супроводжуватися належним навчанням спеціалістів галузі, адміністрації, співробітників, користувачів за дотриманням ними всіх встановлених правил [11].

Тому нашим завданням є розкрити дослідження науковців світу із захисту інформації в системі кібербезпеки та методи здійснення дій проти системи кібербезпеки, які можуть призвести до порушення основних сервісів, наприклад: цілісності, конфіденційності, до-

 DOI 10.34132/pard2025.27.12

ступності, надійності інформації. Вони проявляються в різних формах і за певними ознаками належать до того чи іншого кластеру [9; 10]. Розглянемо основні методи дослідження, які обрали вчені для вивчення цього питання. Серед них є метод використання теорії нечітких відношень, який полягає в математичному обчисленні даних, одержаних при ранжуванні загроз та його практичному застосуванні. До складу дослідників з використання теорії нечітких відношень у ранжуванні загроз захисту інформації в системі кібербезпеки входив автор цієї статті [11].

Науковцями було обрано реальну соціально-економічну систему з власною системою кібербезпеки та елементами інформаційної безпеки для влучного прикладу результатів дослідження, зокрема, кампанію «Sigma Software». Даний об'єкт надає послуги з IT консалтингу у всьому світі, має свої офіси в 14 містах 5-х країн світу – Україні, Польщі, Швеції, США, Австралії у сферах телекомунікацій, реклами, авіації, автомобільній індустрії, фінансів тощо. Вона є частиною «Sigma Group», однієї з найбільших Скандинавських IT-корпорацій, має понад 5000 співробітників, з яких 1500 працювали до 24 лютого 2022 року в Україні.

Відповідно до мети та завдань статті здійснимо стислий опис експертного методу дослідження, яке проводилося науковцями із залученням експертів компанії «Sigma Software» та фахівців з інформаційної та кібербезпеки, які були відібрані науковцями за певними видами індикаторів (критеріїв) [11]. Однак їхня оцінка вважається суб'єктивною і суттєво не вплинула на результати дослідження.

За допомогою експертного методу вченим вдалося ідентифікувати найбільш важливі з суб'єктивного погляду експертів загрози інформаційній безпеці в системі кібербезпеки «Sigma Software», до яких належать [11]:

1) природні явища та техногенний негативний вплив;
2) військове вторгнення;
3) терористичний вплив;
4) промислове шпигунство;
5) хакерський вплив;
6) інсайдерський вплив;

7) безпека каналів зв'язку соціально-економічної системи;

8) ненадійність компонентів безпеки сервісних систем;

9) незахищеність баз даних і хмарних сервісів;

10) небезпека Інтернет-ресурсів;

11) шкідливі програми;

12) DoS-атаки.

В результаті дослідження були визначені вказані вище 12 загроз, які виражаються в порушенні таких критеріїв інформаційної безпеки Sigma Software як [21]:

– доступність інформації;
– цілісність інформації;
– конфіденційність інформації;
– надійність інформації.

Вони утворили набір критеріїв, які вчені за допомогою методу дерева декомпозиції використали для здійснення математичних розрахунків відображення ранжування загроз інформації в системі кібербезпеки однієї соціально-економічної системи [21].

За допомогою математично-статичного методу дослідження, поданого в статті «Ранжування загроз для визначення вартості захисту інформації в середовищі кібербезпеки», автори здійснили ранжування виявлених загроз інформаційній безпеці в системі кібербезпеки обраного ними об'єкта «Sigma Software». Можливо, результати ранжування, визначені ними, не зовсім точні та мають певну похибку, але, поряд із вищезазначеним, основною тезою їх наукового дослідження є демонстрація дієвості та ефективності представлених підходів для вирішення таких проблем.

В цілому, таке дослідження дало змогу вченим визначити допустиму інтенсивність зниження рівня інформаційної безпеки в системі кібербезпеки «Sigma Software», а також витрати на забезпечення безпеки інформації в системі кібербезпеки «Sigma Software». Практичний ефект цього методу дослідження полягав в тому, що він зможе сприяти своєчасному впровадженню ефективних механізмів протидії загрозам, раціональному перерозподілу сил і засобів їх нейтралізації. Таке дослідження є одним з перших щодо значимості практичної спрямованості його результатів у системі

 DOI 10.34132/pard2025.27.12

кібербезпеки й розглядається нами як пріоритетний напрям стратегії реалізації державних механізмів захисту національних цінностей в Україні [19].

Доцільно зазначити, що існують ряд досліджень в цій сфері діяльності, здійснені такими науковцями як О. Силкін, М. Криштанович, А. Зачепа, С. Білоус, А. Красько, S. Musman, AJ. Turner, М. Думчиков, М. Уткіна, О. Бондаренко, Дж. Мартінес, Дж. Дуран, які розглядають й інші методи впливу загроз на систему кібербезпеки, пов'язані з якісною, кількісною та змішаною оцінкою інформаційних ризиків. Розглядаючи ряд моделей для оцінки ризиків системи кібербезпеки нами встановлено, що більшість із методів мають нечітку логіку, їхні моделі вимагають складних розрахунків і тривалого часу для обробки необхідних даних, тоді як оцінка ризиків найчастіше здійснюється лише на рівні активів, а їх вплив на функціонування досліджуваної системи не враховується [12; 13; 14; 15; 16].

В наукових працях О. Гордєєва, В. Харченка, О. Ілляшенка, О. Морозової, М. Гасанова використовується технологія відстеження очей (ЕТТ) для вирішення маркетингових досліджень, оцінки якості користувальницьких інтерфейсів, розробки симуляторів для операторів тощо. У своїй праці «Концепція використання технології відстеження очей для оцінки та забезпечення кібербезпеки, функціональної безпеки та зручності використання» на основі математичної моделі вони розглядають можливість використання цієї технології для вирішення проблеми ідентифікації особистості людини, де розраховується фокус уваги людини і, відповідно, будується візуальний маршрут користувача. Розгадка досягається шляхом відтворення певної траєкторії зором людини. Ця технологія може бути використана як основна або додаткова методика ідентифікації особистості людини [6].

Б. Факіха в подібних дослідженнях пропонує модель оцінки рівня інформаційної безпеки на основі когнітивного підходу, що спрощує обчислення та скорочує час обробки інформації, що надходить. Такий метод моделювання може паралельно використовуватися для навчання спеціалістів працювати в умовах глобалізаційних викликів та загроз [17].

Пропонують покращити видимість вхідних даних для забезпечення захисту кібербезпеки, здійснюючи сценарне моделювання Дж. Сінгх, Т. Паск'є, Дж. Бекон, Х. Ко, Д. Еєрс, D. Tamburri, M. Miglierina, Di Nitto [18; 20]. В результаті їхньої пропозиції застосовування сценарного моделювання визначається рівень безпеки самої системи. Всі методики досліджень загроз захисту інформації в системі кібербезпеки, які доцільно розглядати як стратегічні пріоритети реалізації державних механізмів захисту національних цінностей в Україні, подано в таблиці 1.

Таблиця 1.

Аналіз методик досліджень загроз захисту інформації в системі кібербезпеки

Автори	Концепти наукових праць	Наукові праці
1	**2**	**3**
Добровінський А. Ільченко О. В. Кузьменко С. Чумак В. В. Шелухін О.	економічні та правові аспекти кіберзлочинів у системі Інтернет-банкінгу	Ilchenko, O.V., Chumak, V.V., Kuzmenko, S., Shelukhin, O., Dobrovinskyi, A.V. (2019). Fishing as a cybercrime in the Internet banking system: economic and legal aspects. Journal of Legal, Ethical and Regulatory, 22(2): 6.
Чоудхурі Н. Ністад Е. Регорд, К. Гкіулос, В.	навчання з кібербезпеки в норвезьких компаніях критичної інфраструктури	Chowdhury, N., Nystad, E., Reegård, K., Gkioulos, V. (2022). Cybersecurity training in Norwegian critical infrastructure companies. International Journal of Safety and Security Engineering, 12(3): 299-310
Єманов В. Пасічник В. Євтушенко І Ларін С. Михайленко О.	визначення вартості захисту інформації в середовищі кібербезпеки	Vladislav Emanov, Vasyl Pasichnyk, Ihor Yevtushenko, Stanislav Larin, Olena Mykhailenko (2023). Ranking Threats to Determine the Cost of Protecting Information in a Cybersecurity Environment. Ingénierie des Systèmes d'Information Vol. 28, No. 1, February, pp. 77-84

 DOI 10.34132/pard2025.27.12

продовження таблиці 1

Ємельянов В. Никоненко У. Ситник Ю. Охріменко І. Шульга А.	модель протидії інформаційно-технічним загрозам управління інтелектуальним капіталом інноваційно-орієнтованих систем машинобудівної сфери	Yemelyanov, V., Nikonenko, U., Sytnyk, Y., Okhrimenko, I., Shulga, A. (2022). A model for countering the information and technical threats of intellectual capital management of innovation-oriented systems in the engineering sector. Ingénierie des Systèmes d'Information, 27(5): 799-806
Криштанович М. Філіппова В. Губа М. Карташова О. Молнар О.	оцінка впровадження циркулярної економіки в країнах ЄС у контексті сталого розвитку	Kryshtanovych, M., Filippova, V., Huba, M., Kartashova, O., Mol-nar, O. (2020). Evaluation of the implementation of the circular economy in EU countries in the context of sustainable development. Business: Theory and Practice, 21(2): 704-712.
Гордєєв О. Харченко В. Ілляшенко О. Морозова О. Гасанов М.	технологія відстеження очей для оцінки та забезпечення кібербезпеки, функціональної безпеки та зручності використання	Gordieiev, O., Kharchenko, V., Illiashenko, O., Morozova, O., Gasanov, M. (2021). Concept of using eye tracking technology to assess and ensure cybersecurity, functional safety and usability. International Journal of Safety and Security Engineering, 11(4): 361-367
Lainjo B.	безпека мережі та її вплив на керування програмами	Lainjo, B. (2020). Network security and its implications on program management. International Journal of Safety and Security Engineering, 10(6): 739-746.
Musman S. Turner AJ	ігровий підхід до мінімізації ризиків кібербезпеки	A game oriented approach to minimizing cybersecurity risk. International Journal of Safety and Security Engineering, 8(2): 212- 222

продовження таблиці 1

Думчиков М. Уткіна М. Бондаренко О.	порівняльний аналіз кіберзлочинності як загрози національній безпеці країн Балтії та України	Cybercrime as a threat to the national security of the Baltic States and Ukraine: The comparative analysis. International Journal of Safety and Security Engineering, 12(4): 481-490
Мартінес Дж. Дуран Дж. М.	загроза глобальній кібербезпеці	Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study. International Journal of Safety and Security Engineering, 11(5): 537-545

Джерело: сформовано автором

Перелік досліджень можна продовжити, це ще раз підтверджує актуальність та значимість питання інформаційних загроз у системі кібербезпеки. Однак, увага, зосереджена на ранжуванні інформаційних загроз у системі кібербезпеки із застосуванням теорії нечітких відношень, визначає більш точно рівень захисту та його вартості в системі кібербезпеки і може бути рекомендований до стратегічних пріоритетів реалізації державних механізмів захисту національних цінностей в Україні.

Висновки. Підсумовуючи результати досліджень загроз захисту інформації в системі кібербезпеки як одного зі стратегічних пріоритетів реалізації державних механізмів захисту національних цінностей в Україні, зазначимо, що нині науковці віддали переваги методу теорії нечітких зв'язків, який апробували на окремо обраному для дослідження об'єкту «Sigma Software». Вони визначили практичний ефект цього методу дослідження, яке полягає в тому, що зможе сприяти своєчасному впровадженню ефективних механізмів протидії загрозам, раціональному перерозподілу сил і засобів їх нейтралізації. На основі певних рангів множину загроз розбили на кластери, які не перетинаються і еквівалентні за вагою. Для забезпечення безпеки досліджуваних систем було

 DOI 10.34132/pard2025.27.12

запропоновано розподіл допустимих витрат пропорційно рангам загроз, що сприятиме раціональному використанню ресурсів і засобів запобігання, усунення або зменшення впливу можливих загроз кібербезпеці.

Запропоновано також інші методи оцінки впливу загроз на рівень кібербезпеки, пов'язані з якісною, кількісною та змішаною оцінкою інформаційних ризиків, які також можуть ввійти до складу стратегічних пріоритетів реалізації державних механізмів захисту національних цінностей в Україні.

Доцільно зазначити, що описані методи оцінки впливу загроз на рівень кібербезпеки сприяють прогнозувати розвиток ситуації в умовах глобалізаційних викликів та загроз з метою прийняття своєчасних та ефективних управлінських рішень, спрямованих на підвищення безпеки самої інформації в системі кібербезпеки. Також виникає потреба звернути увагу на визначення впливу найбільш значущих концептів нечіткої когнітивної картини на безпеку інформації як такої в системі кібербезпеки обраного об'єкта в різні моменти часу.

ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМІ КІБЕРБЕЗПЕКИ ЯК СТРАТЕГІЧНИЙ ПРІОРИТЕТ РЕАЛІЗАЦІЇ ДЕРЖАВНИХ МЕХАНІЗМІВ ЗАХИСТУ НАЦІОНАЛЬНИХ ЦІННОСТЕЙ В УКРАЇНІ

В статті здійснено аналіз досліджень загроз захисту інформації в системі кібербезпеки, які автор розглядає як стратегічний пріоритет реалізації державних механізмів захисту національних цінностей в Україні.

Методологією дослідження є метод ранжування загроз захисту інформації в системі кібербезпеки, який відображений через теоричні засади та метод експертно-дослідницьких зв'язків. Автор акцентує увагу на сучасні методи захисту інформації в системі кібербезпеки щодо реалізації державних механізмів захисту національних цінностей в Україні. Отримані вченими результати дозволили виокремити перелік загроз у системі кібербезпеки задля

формування інформаційної основи з прийняття та реалізації управлінських рішень.

Мета статті – на основі теоретико-методологічного аналізу наукової літератури виокремити загрози захисту інформації в системі кібербезпеки як одного з стратегічних пріоритетів реалізації державних механізмів захисту національних цінностей в Україні в умовах воєнного стану та перспектив трансформаційних змін у державному управлінні у післявоєнний період України.

Результати, отримані науковцями в цій сфері діяльності, мають практичне та наукове значення: завдяки використанню методичного підходу до формування вимог до захисту інформації в системі кібербезпеки розглядаються сегменти стратегічних пріоритетів захисту національних цінностей в Україні. Виокремлені методи, які автор демонструє для досягнення поставленої мети, зокрема, метод аналізу стану забезпечення кібербезпеки та методи опису й класифікації, сприяють здійсненню ефективному захисту інформації як одного зі стратегічних пріоритетів з реалізації державних механізмів захисту національних цінностей в Україні.

Методологічний підхід визначає, що доцільно здійснити опис, і лише потім – класифікацію різних видів загроз і небезпек, ризиків і викликів і, відповідно, сформулювати систему заходів щодо управління ними

В якості поширених методів аналізу рівня забезпечення кібербезпеки використовуються методи дослідження причинно-наслідкових зв'язків між загрозами та небезпеками; здійснюється пошук причин, що стали джерелом і призвели до актуалізації окремих факторів небезпек. Запропоновані заходи щодо нейтралізації загроз захисту інформації в системі кібербезпеки як одного зі стратегічних пріоритетів реалізації державних механізмів захисту національних цінностей в Україні.

Ключові слова: *державні механізми захисту національних цінностей в Україні, стратегічні пріоритети реалізації державних механізмів, загрози захисту інформації, система кібербезпеки, воєнний стан, трансформаційні зміни у державному управлінні.*

 DOI 10.34132/pard2025.27.12

Author Contributions: Conceptualization, B.W.A. and L.W.F.; Writing – original draft, B.W.A. and L.W.F.; Writing – review & editing, B.W.A. and L.M.F. Author has read and agreed to the published version of the manuscript.
Funding: This research received no external funding.
Institutional Review Board Statement: Not applicable as study did not include human subjects.
Informed Consent Statement: Not applicable.
Data Availability Statement: Data is contained within the article.
Conflicts of Interest: The author declares no conflict of interest.

References

1. Ilchenko, O., Chumak, V., Kuzmenko, S., Shelukhin, O., & Dobrovinskyi, A. (2019). Fishing as a cybercrime in the Internet banking system: economic and legal aspects. *Journal of Legal, Ethical and Regulatory*, 22(2), (pp. 1-6). Retrieved from: https://dspace.univd.edu.ua/server/api/core/bitstreams/5a768643-b341-4db2-84dd-65311c55eb48/content [in English].

2. Chowdhury, N., Nystad, E., Reegård, K., & Gkioulos, V. (2022). Cybersecurity training in Norwegian critical infrastructure companies. *International Journal of Safety and Security Engineering*, 12(3), (pp. 299-310). Retrieved from: https://doi.org/10.18280/ijsse.120304 [in English].

3. Yemelyanov, V., Nikonenko, U., Sytnyk, Y., Okhrimenko, I., & Shulga, A. (2022). Model of countering information and technical threats to intellectual capital management of innovation-oriented systems in the machine-building sector. *Ingénierie des Systemes d'Information*, 27(5), (pp. 799-806). Retrieved from: https://doi.org/10.18280/isi.270513 [in English].

4. Kryshtanovych, M., Filippova, V., Huba, M., Kartashova, O., & Molnar, O. (2020). Assessment of the implementation of the circular economy in EU countries in the context of sustainable development. *Business: theory and practice*, 21(2), (pp. 704-712). Retrieved from: https://doi.org/10.3846/btp.2020.12482 [in English].

5. Kryshtanovych, M., Petrovskyi, P., Khomyshyn, I., Bezena, I., & Serdechna, I. (2020). Peculiarities of the implementation of governance in the social protection system. *Business, Management and Economics Engineering*, 18(1), (pp. 142-156). Retrieved from: https://doi.org/10.3846/bme.2020.12177 [in English].

6. Kryshtanovych, S., Liubomudrova, N., Tymofieiev, S., Shmyhel, O., & Komisarenko, A. (2022). Modeling ways to counter external threats to corporate security of machine-building enterprises in the context of COVID-19. *International Information and Engineering Technology Association*, 12(2), (pp. 217-222). Retrieved from: https://doi.org/10.18280/ijsse.120210 [in English].

7. Magruk, A. (2016). Uncertainty in the field of Industry 4.0 – potential directions for research. *Business, Management and Economic Engineering*, 14(2), (pp. 275-291). Retrieved from: https://doi.org/10.3846/bme.2016.332 [in English].

8. Gordieiev, O., Kharchenko, V., Illiashenko, O., Morozova, O., & Gasanov, M. (2021). The concept of using eye tracking technology to assess and ensure cybersecurity, functional safety and usability. *International Information and Engineering Technology Association*, 11(4), (pp. 361-367). Retrieved from: https://doi.org/10.18280/ijsse.110409 [in English].

9. Lainjo, B. (2020). Network security and its implications on program management. *International Information and Engineering Technology Association*, 10(6), (pp. 739-746). Retrieved from: https://doi.org/10.18280/ijsse.100603 [in English].

10. Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: Perspectives and challenges. *Wireless Networks*, 20, (pp. 2481-2501). Retrieved from: https://doi.org/10.1007/s11276-014-0761-7 [in English].

11. Emanov, V., Pasichnyk, V., Yevtushenko, I., Larin, S., & Mykhailenko, O. (2023). Ranking Threats to Determine the Cost of Protecting Information in a Cybersecurity Environment. *Ingénierie des Systemes d'Information*, (Vol. 28), 1, (pp. 77-84). Retrieved from: https://doi.org/10.18280/isi.280108 [in English].

12. Sylkin, O., Shtanhret, A., Ohirko, O., & Melnykov, A. (2018). Assessing the financial security of the engineering enterprises as preconditions of application of anti-crisis management. *Business and Economic Horizons*, 14 (4), (pp. 926-940). Retrieved from: https://doi.org/10.15208/beh.2018.63 [in English].

13. Sylkin, O., Kryshtanovych, M., Zachepa, A., Bilous, S., & Krasko, A. (2019). Modeling the process of applying anti-crisis management in the system of ensuring financial security of the enterprise. *Business: theory and practice*, 20, (pp. 446-455). Retrieved from: https://doi.org/10.3846/btp.2019.41 [in English].

14. Musman, S., & Turner, A. (2018). A game oriented approach to minimizing cybersecurity risk. *WIT Press*, 8(2), (pp. 212-222). Retrieved from: https://doi.org/10.2495/SAFE-V8-N2-212-222 [in English].

15. Dumchykov, M., Utkina, M., & Bondarenko, O. (2022). Cybercrime as a Threat to the National Security of the Baltic States and Ukraine. *International Information and Engineering Technology Association*, 12(4), (pp. 481-490). Retrieved from: https://doi.org/10.18280/ijsse.120409 [in English].

16. Leukfeldt, E., Lavorgna, A., & Kleemans, E. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research*, 23(3), (pp. 287-300). Retrieved from: https://doi.org/10.1007/s10610-016-9332-z [in English].

17. Martínez, J., & Durán, J. (2021). Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study. *International Information and Engineering Technology Association*, 11(5): 537-545. https://doi.org/10.18280/ijsse.110505 [in English].

18. Fakiha, B. (2021). Business organization security strategies to cyber security threats. *International Information and Engineering Technology Association*, 11(1), (pp. 101-104). Retrieved from: https://doi.org/10.18280/ijsse.110111 [in English].

19. Yemelyanov, V., & Bondar, H. (2019). Kiberbezpeka yak skladova natsionalnoi bezpeky ta kiberzakhyst krytychnoi infrastruktury ukrainy. *Publichne upravlinnia ta rehionalnyi rozvytok – Public Administration and Regional Development*, (5), (pp. 493-523). Retrieved from: https://doi.org/10.34132/pard2019.05.02

20. Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D. (2016). Twenty security considerations for cloud-supported Internet of Things. *IEEE Internet of Things Journal*, 3(3), (pp. 269-284). Retrieved from: https://doi.org/10.1109/JIOT.2015.2460333 [in English].

21. Tamburri, D.A., Miglierina, M., & Di Nitto, E. (2020). Cloud applications monitoring: An industrial study. *Information and Software Technology*, 127. Retrieved from: https://doi.org/10.1016/j.infsof.2020.106376 [in English].

Відомості про автора / Information about the Author

Станіслав Ларін, к. н. з держ. упр., доцент кафедри державного управління Навчально-наукового інституту державного управління та державної служби Київського національного університету імені Тараса Шевченка, м. Київ, Україна. E-mail: larin.stan@gmail.com, orcid: https//orcid.org/0000-0001-8544-7714.

Stanislav Larin, Candidate of Sciences in Public Administration, Associate Professor, Department of Public Administration, Educational and Scientific Institute of Public Administration and Civil Service, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine. E-mail: larin.stan@gmail.com, orcid: https//orcid.org/0000-0001-8544-7714.

Larin, S. (2025). Protection of information in the cybersecurity system as a strategic implementation priority for state mechanisms of national values protection in Ukraine. Public Administration and Regional Development, 27, 278-294. https://doi.org/10.34132/pard2025.27.12