DOI: 10.58254/viti.8.2025.09.117

УДК 004.056

канд. техн. наук Мазулевський О. Є. ORCID: 0000-0002-6042-2577 (ВІТІ ім. Героїв Крут)
д-р філософії Зарубенко А. О. ORCID: 0000-0002-7616-6416 (ВІТІ ім. Героїв Крут)
канд. техн. наук Коваленко І. Г. ORCID: 0000-0002-6827-5196 (ВІТІ ім. Героїв Крут)

ВИЯВЛЕННЯ КРИТИЧНИХ ЗМІН У ДИНАМІЦІ КІЛЬКОСТІ КІБЕРІНЦИДЕНТІВ ЯК ІНДИКАТОРА ПРОГНОЗУВАННЯ ВИНИКНЕННЯ КРИЗОВИХ СИТУАЦІЙ В ОБОРОННОМУ ВІДОМСТВІ

У статті представлено науково обґрунтований підхід до оцінювання поточного стану кіберстійкості оборонного відомства, заснований на аналізі статистичних даних щодо кількості зареєстрованих кіберінцидентів. Запропонований підхід передбачає використання методів лінійної алгебри та статистичного аналізу для виявлення закономірностей та динамічних змін у розвитку кіберзагроз. Такий підхід дозволяє визначати моменти критичних відхилень, що можуть свідчити про зниження рівня кіберстійкості або підвищення ймовірності настання кризових ситуацій у кіберпросторі. Отримані результати створюють наукове підґрунтя для подальшого вдосконалення процесів оцінювання стану кіберзахисту, прогнозування ризиків та формування ефективної системи прийняття рішень у сфері кібербезпеки оборонного сектору.

Особливу увагу приділено розробленню алгоритмічного підходу до визначення критичних моментів у часових рядах показників кіберінцидентів, що дає змогу швидко реагувати на зміни у рівні загроз та адаптувати заходи кіберзахисту відповідно до поточної ситуації. У роботі підкреслено важливість інтеграції аналітичних методів до системи моніторингу кібербезпеки з метою підвищення ефективності виявлення та запобігання кібератакам.

Дослідження є першим етапом у формуванні комплексного методу оцінювання кіберстійкості та прогнозування ризиків для оборонного відомства відповідно до законодавчо визначеної зони відповідальності, що передбачає подальшу розробку механізмів протидії кризовим явищам у кіберпросторі. Практична значущість результатів полягає у створенні основи для підвищення ефективності управлінських рішень, забезпеченні завчасного виявлення загроз, мінімізації негативних наслідків кібератак та підтриманні належного рівня ситуаційної обізнаності керівного складу Міністерства оборони та Збройних Сил України.

Ключові слова: *кіберстійкість, кібербезпека, криза в галузі кібербезпеки, кіберінцидент.*

O. Mazulevsky., A. Zarubenko, I. Kovalenko. Identification of critical changes in the dynamics of the number of cyber incidents as an indicator for forecasting the occurrence of crisis situations in the defense department

The article presents a scientifically grounded approach to assessing the current state of cyber resilience of the defense agency, based on the analysis of statistical data regarding the number of recorded cyber incidents. The proposed methodology employs methods of linear algebra and statistical analysis to identify patterns and dynamic changes in the development of cyber threats. This makes it possible to determine moments of critical deviation that may indicate a decrease in cyber resilience or an increased likelihood of crisis situations in cyberspace. The obtained results provide a scientific foundation for improving cyber defense assessment processes, risk forecasting, and the development of an effective decision-making framework in the field of cybersecurity for the defense sector.

Special attention is devoted to developing an algorithmic approach for identifying critical moments within time series of cyber incident indicators, enabling timely response to variations in the threat landscape and the adaptive adjustment of cybersecurity measures according to current conditions. The study emphasizes the importance of integrating analytical methods into information security monitoring systems to enhance the efficiency of detecting and preventing cyberattacks.

This research represents the first stage in the development of a comprehensive methodology for assessing cyber resilience and forecasting risks for the defense agency in accordance with its legally defined area of responsibility. It also establishes a basis for further development of mechanisms to counteract crisis phenomena in cyberspace. The practical significance of the results lies in strengthening the effectiveness of managerial decision-making, ensuring early threat detection, minimizing the negative consequences of cyber incidents, and maintaining an adequate level of situational awareness among the leadership of the Ministry of Defense and the Armed Forces of Ukraine.

Keywords: *cyber resilience, cybersecurity, cybersecurity crisis, cyber incident.*

Вступ

Постановка проблеми. У сучасних умовах стрімкого розвитку інформаційних технологій, які проникають у всі сфери життєдіяльності, зокрема у військову, кібербезпека набуває статусу критично важливого чинника стабільного функціонування будь-якої

організації. Захист інформаційних ресурсів від загроз у кіберпросторі є необхідною передумовою ефективної діяльності, оскільки порушення кібербезпеки може призвести до значних фінансових і репутаційних втрат, зупинки процесів управління чи навіть до втрати людських життів у разі військових структур. З огляду на постійне зростання кількості та складності кібератак, перед фахівцями у сфері кібербезпеки постає завдання не лише оперативного реагування на інциденти, а й прогнозування потенційних кризових ситуацій в галузі кібербезпеки з метою мінімізації їх наслідків. У даній статті представлено один із етапів уперше розробленого процесу виявлення та прогнозування виникнення кризових явищ на основі статистичного аналізу даних про зафіксовані кіберінциденти та визначення числової оцінки поточного рівня кіберстійкості оборонного відомства для забезпечення належної ситуаційної обізнаності його керівництва.

Аналіз останніх досліджень та публікацій. Відповідно до [1] передбачено створення ситуаційного центру Кабінету Міністрів, а також ситуаційних центрів центральних органів виконавчої влади, обласних і Київської міської державних адміністрацій, інших державних органів та установ сектору безпеки й оборони, зокрема Міністерства оборони України.

Водночас у вітчизняному науковому та інформаційному просторі відсутні публікації, що висвітлюють методологічні підходи до виявлення потенційно можливих кризових ситуацій у кіберпросторі на основі аналізу статистичних даних. Єдиним нормативним документом, який частково стосується цього питання, є [2]. Проте зазначений документ регламентує лише взаємодію суб’єктів у процесі ліквідації вже наявних кризових ситуацій, не охоплюючи аспектів їх попередження чи прогнозування.

У зв’язку з цим, в тезах доповіді [3] запропоновано розпочати розробку та у даній статті представлено фрагмент *Методу прогнозування та виявлення кризових ситуацій у кіберпросторі на основі обробки статистичних даних*.

Мета статті. Метою статті є представлення підходу оцінювання поточного стану кіберстійкості оборонного відомства з урахуванням ситуації у кіберпросторі на основі статистичного аналізу зафіксованих кіберінцидентів.

Виклад основного матеріалу дослідження

У процесі участі у війні (військових конфліктах) країна та суспільство зазнають стрімкого розвитку в різних галузях, що є запорукою вдалого протистояння ворогу. Однією з основних ознак розвитку сучасного суспільства (зокрема військової організації країни) під час війни є зростання залежності від якості й надійності інформаційно-комунікаційних систем (ІКС), які застосовуються в діяльності в усіх галузях життя: від країни як механізму державності, включно із воєнною організацією, так громадянина як носія державності. Відповідне посилення високорівневої спрямованості розвитку інформаційних ресурсів зумовлює необхідність підвищення вимог до рівня їх інформаційної безпеки, а особливо в умовах військового протиборства.

Проблема ускладнена особливістю глобальної мережі Інтернет, з якою інтегровано більшість ІКС і використанням загальнодоступного програмного забезпечення, призводять до накопичення випадкових і непередбачуваних впливів.

Зазначимо, що ІКС, які мають підключення до Інтернет, розглядаються в ракурсі необхідності захисту ресурсів таких систем від кібератак у процесі реалізації базових технологічних процесів отримання, зберігання, транспортування, оброблення та відображення інформації [4].

Обумовимо, що деякі терміни будуть використовуватися відповідно до [5]:

інформаційна безпека та кібербезпека в інформаційно-комунікаційних системах (інформаційна безпека в ІКС, ІБ в ІКС) − сукупність організаційних, правових, інженерно-технічних заходів, спрямованих на захист інформації та кіберзахист ІКС;

інцидент безпеки інформації – подія або низка несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії

людського фактору) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці ІКС, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку інформації, що обробляється в таких ІКС.

Введемо термін: кіберстійкість ІКС – стан ІКС, за якого забезпечується її спроможність надійно функціонувати та надавати основні послуги в умовах кіберзагроз.

Інші терміни вживаються в значеннях, які наведені в Законах України [6; 7], Державному Стандарті України [8].

Згідно зі статтею 8 Закону України «Про основні засади забезпечення кібербезпеки України» [6] Міністерство оборони України є одним із основних суб’єктів національної системи кібербезпеки і відповідно до компетенції здійснює заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі. Тому, слід мати можливість оцінити стан кіберстійкості ІКС оборонного відомства і державних органів (установ) для прийняття зважених управлінських рішень в мирний час та під час функціонування в особливий період.

Далі, розглянемо отримання даних для проведення оцінки поточного стану системи з урахуванням ситуації у кіберпросторі. Для формування вірної картини стану кіберстійкості доречним буде проведення регулярного моніторингу результатів роботи засобів кіберзахисту в ІКС. Моніторинг реалізується шляхом збору статистичних даних виявлених кіберінцидентів засобами кіберзахисту та за допомогою роботи аналітиків кібербезпеки.

Для оцінки в Міноборони слід збирати дані за базові елементи національної системи кібербезпеки, а саме від державного сектору України, Збройних Сил України та Міністерства оборони України, за можливості інших елементів.

Для проведення оцінки поточного стану з урахуванням ситуації у кіберпросторі стану кіберстійкості Міноборони використовуються наступні показники, які показують рівень напруженості ситуації в кіберпросторі: узагальнений індекс напруженості ситуації у кіберпросторі; індекси напруженості ситуації у кіберпросторі для Державного сектору, ЗС України та Міноборони (усі окремо); узагальнений індекс змін кількості виявлених кіберінцидентів; індекси змін кількості виявлених кіберінцидентів для Державного сектору, ЗС України та Міноборони (усі окремо); композитний показник кіберстійкості (розраховується з урахуванням оцінки забезпеченості кібербезпеки в ІКС відомства, буде запропоновано у подальших дослідженнях).

Визначення узагальненого індексу напруженості ситуації у кіберпросторі і узагальненого індексу змін кількості виявлених кіберінцидентів проводиться на основі статистичних даних кількості виявлених кіберінцидентів у відповідальних підрозділах із кібербезпеки в ІТС та змін кількості кіберінцидентів у поточний момент із врахуванням даних за певний минулий період часу.

Індекс кількості виявлених інцидентів кібербезпеки розраховується для оцінки зміни виявленої активності проти ІКС різної приналежності. Дані, які надходять, мають відповідати Переліку категорій кіберінцидентів, схваленого Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони України [9]. Приклад таксономії переліку категорій та типів кіберінцидентів наведено на сайті CERT-UA [10]. Перелік розроблявся для впровадження структуризації даних для обміну інформацією щодо кіберінцидентів в установах усіх форм власності.

Дані зі звітів по різними типам кіберінцидентів заносяться до таблиці. Для проведення статистичного аналізу необхідно мати вибірку даних не менше визначеного періоду, наприклад за 90 діб. На далі розмір вибірки може змінюватися з наданням обґрунтування.

На основі вибірки розраховуються наступні показники: перцентранк поточних показників за всіма типами кіберінцидентів (використовується для знаходження узагальненого індексу напруженості ситуації у кіберпросторі); середнє геометричне

перцентранка поточних показників за всіма типами кіберінцидентів (використовується для знаходження узагальненого індексу напруженості ситуації у кіберпросторі); кількість верхніх крайніх значень перцентранка поточних показників за всіма типами кіберінцидентів (використовується для знаходження узагальненого індексу змін кількості виявлених кіберінцидентів); кількість нижніх крайніх значень перцентранка поточних показників за всіма типами кіберінцидентів (використовується для знаходження узагальненого індексу змін кількості виявлених кіберінцидентів).

Розглянемо розрахунок індексу напруженості ситуації у кіберпросторі. Узагальнений індекс напруженості ситуації у кіберпросторі розраховується на основі вибору максимального із індексів напруженості ситуації у кіберпросторі для окремих елементів, зокрема для ІКС Міноборони, ЗСУ, Держсектору, розрахунок яких розглянемо далі в матеріалах статті.

Розрахунок індексу напруженості ситуації у кіберпросторі для різних відомств проводиться за однаковими принципами але за своїми статистичними даними взятими зі звітів по напрямкам шляхом визначення перцентранку для кожного дня.

Перцентранк – перцентильний ранг значення у масиві даних (зворотна функція перцентиля). *Перцентиль* – значення ознаки, яке відокремлює кожну соту частину впорядкованого ряду, указує на відносне місце визначеного значення в загальному розподілі впорядкованої множини.

Функція розрахунку перцентраку обчислює перцентильний ранг значення (x) у масиві даних $\{A\}$. Формула для обчислення виглядає наступним чином:

$$P(x)=(r-1)/(N-1), \quad (1)$$

де $P(x)$ – перцентильний ранг значення x;

r – ранг значення x у впорядкованому масиві $\{A\}$;

N – загальна кількість елементів у масиві $\{A\}$.

Порядок розрахунку:

1. Впорядкування масиву: спочатку впорядковується масив даних $\{A\}$ у порядку зростання.

2. Визначення рангу: знаходиться ранг r значення x у впорядкованому масиві. Ранг – це позиція значення x у масиві $\{A\}$, починаючи з першого найменшого значення.

3. Обчислення перцентильного рангу: використовуючи формулу (1), де N – загальна кількість елементів у масиві, обчислюється перцентильний ранг значення x.

Обчислення проводиться для кожного типу кіберінцидентів (КІ) за визначений період і буде визначати множину $\{_{date}Perc\}$ набору перцентранків кожного відліку (за датою).

Наступним етапом розрахунків є знаходження середнього геометричного перцентранка поточних показників за всіма типами кіберінцидентів, що і буде значенням *індексу напруженості ситуації у кіберпросторі для елементу спостереження* (МО України, ЗС України, Держсектору). Для цього скористаємося класичною формулою розрахунку середнього геометричного: *середнє геометричне* (середнє пропорційне) декількох додатних чисел дорівнює кореню, ступінь якого дорівнює кількості чисел, із добутку даних чисел. Значення узагальнюється на довільну кількість чисел більших нуля. Середнє геометричне E чисел $a_1, a_2 \ldots a_E$ дорівнює кореню E-го ступеня із добутку даних чисел. Середнє геометричне E чисел $a_1, a_2 \ldots a_E$ дорівнює

$$Risk\_index = \sqrt[E]{\prod_{e=1}^{E} a_e}\ , \quad (2)$$

де E – кількість додатніх значень перцентранка за типами кіберінцидентів; a_e –додатні значення перцентранка за типами кіберінцидентів.

Індекс напруженості ситуації у кіберпросторі розраховується для кожного напряму спостереження, а саме для Міноборони, Збройних Сил України, державного сектору України.

Узагальнений індекс напруженості ситуації у кіберпросторі, як зазначалося вище, визначається вибором максимального значення серед індексів напруженості кожного напрямку спостереження.

Максимальне значення використовується з розуміння того, що відсутність проведення (виявлення) кіберінцидентів в одному із напрямів спостереження не є основою для припущення послаблення напруженості у кіберпросторі.

Індекс змін кількості виявлених кіберінцидентів. Подальшим етапом обробки статистичних даних є *знаходження верхніх крайніх та нижніх крайніх значень перцентранку кількості кіберінцидентів за типами, для кожного напрямку*. Порогові значення визначаються емпіричним шляхом (в подальшому можуть змінюватися для детального налаштування моделі прогнозування). На першому етапі прийнято рішення про фіксацію таких випадків:

для фіксації низького рівня кількості кіберінцидентів виражених перцентранком за типами при зменшенні менше ніж порогове значення;

для фіксації високого рівня кількості кіберінцидентів виражених перцентранком за типами при перебільшенні більше ніж порогове значення.

Використання декількох рівнів порогових значень може застосовуватися для визначення ступеню впливу та побудови більш точних моделей виявлення кіберінцидентів та прогнозування різних типів кібератак (кібервпливів) і в подальшому настання, на їх основі, кризових ситуацій. Для кожного окремого напряму розраховується значення кількості значень подолання порогових значень, в яких значення перераховані від більш суворих до більш м'яких.

Для кожного напряму визначимо кількість спрацювань по кожному пороговому значенню у матриці кількості подолань порогів [$_{date}B$] згідно з виразом:

$$_{date}B = \begin{bmatrix} |\forall \{_{date}Perc_{k=1..|_{date}Perc|}\} \leq MinPor_{p=1..P}|; \\ |\forall \{_{date}Perc_{k=1..|_{date}Perc|}\} \geq MaxPor_{p=1..P}|; \end{bmatrix},$$

де $_{date}Perc_{k=1..|_{date}Perc|}$ – усі елементи множини значень перцентранків кількості кіберінцидентів за визначену дату;

MinPor – матриця значень мінімальних порогових значень;

MaxPor – матриця значень максимальних порогових значень.

Отже, в матриці кількості подолання порогів [$_{date}B$] визначаються кількість зменшень відносно мінімальних порогів в першому рядку та кількість перебільшень максимальних порогів в другому рядку.

Подолання порогового значенням перцентранку кількості кіберінцидентів за типами дає змогу побачити аномальну активність/безактивність зловмисників. Перевищення покаже ймовірний початок нової атаки (етапу атаки), а заниження про завершення атаки (етапу атаки) і підготовку до нової атаки (етапу атаки). Як відомо, кібератака складається із декількох етапів, про що можливо дізнатися із різних підходів вивчення кібератак. Так, наприклад, «Cyber Kill Chain» від Lockheed Martin поділяє кібератаку на 7 етапів [11], а «MITRE ATT&CK» на 14 «тактик» із описом конкретних «технік» [12] для реалізації різних типів кібератак.

Не всі етапи кібератаки призводять до підвищення значень кількості кіберінцидентів, не всі атаки використовують послідовність класичних моделей та можуть бути проведені в повному обсязі набору дій в моделі для досягнення поставлених цілей (у разі дії не фінансово вмотивованих зловмисників, а політично чи примусово…). Або кібератаки різного типу

можуть бути етапами однієї більшої скоординованої кібератаки. Наприклад, останнім часом, ворогом, (через використання APT-угрупувань, Advanced Persistent Threat) під час проведення атак на інфраструктуру державного сектору для відволікання уваги фахівців кібербезпеки та/або переведення телекомунікаційного обладнання в критичні режими функціонування, проводяться атаки розподіленої відмови в обслуговуванні (DDoS) з залученням контрольованих «хактивістів» (політично або ідеологічно вмотивованих кіберзлочинців здебільшого із низьким рівнем підготовки) країни агресора під різними вигаданими (надуманими) приводами. Отже, «хактивісти» вважають це проведенням окремого «акту впливу» (помсти, покарання), а насправді є інструментом на черговому етапі для більш скоординованої кібератаки.

Індекс змін кількості виявлених кіберінцидентів розраховується окремо за кожним напрямом Міноборони, Збройних Сил України, державного сектору України, тощо. Для його знаходження використаємо раніше визначену матрицю кількості подолання порогів [$_{date}B$] відповідно для кожного напряму:

$$divIncidents = ({}_{date}B_{1,1} + {}_{date}B_{2,1}) * q,$$

де $_{date}B_{1,1}$ – елемент матриці $[_{date}B]$, який показує кількість подолання мінімального порогу (1 рядок 1 стовпець);

$_{date}B_{2,1}$ – елемент матриці $[_{date}B]$, який показує кількість подолання найстрогішого максимального порогу (2 строка 1 стовпець);

q – рівнозважений коефіцієнт впливу подолання порогового значення.

Значення рівнозваженого коефіцієнту впливу спрацювання порогового значення визначається як: $q = 100\% / 21 \approx 4.76$, де 21 – кількість типів кіберінцидентів в таксономії [10]. Значення рівнозваженого коефіцієнту впливу спрацювання порогового значення в подальшому можливо змінювати використовуючи наукові підходи, наприклад, методом парних порівнянь.

Узагальнений Індекс змін кількості виявлених кіберінцидентів визначається як максимальне значення серед індексів змін кількості виявлених кіберінцидентів кожного напряму спостереження.

Максимальне значення використовується з розуміння того, що відсутність проведення (виявлення) кіберінцидентів в одному з напрямів спостереження не є основою для припущення послаблення напруженості у кіберпросторі.

У подальшому для загальної картини варто розрахувати композитний показник кіберстійкості. Але для його оцінки потрібно оцінити результати впровадження заходів та засобів кіберзахисту в інфраструктурі відомств. Розгляд способу згаданої оцінки буде розглянуто в подальших дослідженнях.

В загальному, розробка *Методу прогнозування та виявлення кризових ситуацій у кіберпросторі на основі обробки статистичних даних* оборонного відомства, ґрунтується на трьох послідовних етапах:

оцінювання забезпеченості системи кібербезпеки нормативно-правовими документами, їх змістовому наповненню та наявності технічних засобів кіберзахисту (є напрямом подальших досліджень);

аналіз поточного стану на основі статистичних даних щодо кількості та типів зафіксованих кіберінцидентів (розглянуто у даній статті);

прогнозування можливих кризових ситуацій у кіберпросторі з метою своєчасного реагування та мінімізації їх наслідків (є напрямом подальших досліджень).

Реалізація зазначеного методу сприятиме підвищенню спроможності оборонного відомства протидіяти кіберзагрозам шляхом запровадження ефективних заходів попередження та реагування.

Висновки й перспективи подальших досліджень

Запропонований у статті підхід до оцінювання поточного стану кіберстійкості оборонного відомства дає змогу підвищити рівень ситуаційної поінформованості щодо характеру та інтенсивності впливу противника (зловмисників) у кіберпросторі, а також слугує індикатором можливого наближення кризових ситуацій у сфері кібербезпеки. Представлений спосіб є складовою частиною "Методу прогнозування та виявлення кризових ситуацій у кіберпросторі на основі обробки статистичних даних", подальша розробка й удосконалення якого визначають напрям наступних досліджень.

Впровадження оцінки поточного стану та прогнозування виникнення кризових ситуацій дозволить виявити прогалини в організації та забезпеченні кібербезпеки, ідентифікувати ознаки формування кризових ситуацій, що, в свою чергу, підвищить рівень готовності відомства до реагування на них, чим буде досягнуто мінімізації наслідків кіберінцидентів та забезпечення стабільного функціонування ІКС. Таким чином, розробка і практичне застосування зазначеного Методу становлять важливий крок до зміцнення кіберстійкості оборонного відомства в умовах зростаючої активності кіберзлочинців, державно-вмотивованих APT-груп і появи нових загроз у кіберпросторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Питання мережі ситуаційних центрів: Постанова Кабінету Міністрів України від 11.07.2023 № 705. URL: https://zakon.rada.gov.ua/laws/show/705-2023-%D0%BF#Text (дата звернення: 24.11.2025).

2. Порядок взаємодії суб’єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки, затверджений Національним координаційним центром кібербезпеки 22.09.2022. URL: https://www.rnbo.gov.ua/ua/Diialnist/5765.html (дата звернення: 24.11.2025).

3. Мазулевський О., Денесюк Р. Прогнозування та виявлення кризових ситуацій у кіберпросторі на основі обробки статистичних даних // Тези доповідей Науково-практичної конференції «Інформаційно-аналітичне забезпечення органів військового управління: Проблемні питання та шляхи їх вирішення» НУОУ, 28.11.2024 р. С. 74–75.

4. Терейковський І., Корченко А. Інтелектуалізовані методи захисту інформації: нейронні мережі в захисті інформації : навч. посіб. КПІ ім. Ігоря Сікорського, 2022. 175 с.

5. Основні засади забезпечення інформаційної безпеки та кібербезпеки в інформаційно-комунікаційних системах: затверджено Наказом Міністерства оборони України від 18.04.2024 № 248.

6. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 24.11.2025).

7. Про захист інформації в інформаційно-комунікаційних системах: Закон України (зі змінами) від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/ laws/show/80/94-%D0%B2%D1%80#Text.

8. Державний Стандарт України ISO/IEC 27000:2023. Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів. Наказ ДП «УкрНДНЦ» від 17.08.2023 № 210.

9. Протокол № 18 засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України від 25.10.2021 (від 28.10.2021 № 16/320/21).

10. Перелік категорій кіберінцидентів. URL: https://cert.gov.ua/recommendation/ 16904 (дата звернення: 24.11.2025).

11. The Cyber Kill Chain® framework. Lockheed Martin. 2024. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (дата звернення: 24.11.2025).

12. Globally-accessible knowledge base of adversary tactics and techniques MITRE ATT&CK®. 2024. URL: https://attack.mitre.org/ (дата звернення: 24.11.2025).