УДК 004.056.53
DOI https://doi.org/10.32689/maup.it.2025.3.19

Олександр ПОПОВ
член-кореспондент НАН України, доктор технічних наук, професор, директор,
Центр інформаційно-аналітичного та технічного забезпечення моніторингу об'єктів атомної енергетики НАН України,
професор кафедри комп'ютерних інформаційних систем і технологій,
ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом»,
sasha.popov1982@gmail.com
***ORCID:** 0000-0002-5065-3822*

Роман ДРАГУНЦОВ
аспірант,
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України,
draguntsow@yahoo.com
***ORCID:** 0000-0002-1781-7530*

КЛЮЧОВІ ВИКЛИКИ ДЛЯ ОПЕРАЦІЙНИХ ЦЕНТРІВ КІБЕРБЕЗПЕКИ В УМОВАХ ПОВНОМАСШТАБНОЇ ВІЙНИ

Анотація. *У статті систематизовано ключові чинники, що визначають ефективність комерційних і державних Security Operation Center (SOC) України в 2022–2025 рр.: деградація енергетичної та телекомунікаційної інфраструктури, окупація й фізична втрата ІТ-активів, кібервійна державного рівня, кадрова криза та перехідна розрізненість регуляторних норм.*

Мета. *Визначити та оцінити вплив обмежень середовища на роботу SOC в умовах сучасної повномасштабної війни, визначити ключові особливості загроз кібербезпеки в даних умовах.*

Методологія. *У дослідженні застосовано комбінований підхід, що поєднує огляд та аналіз існуючих досліджень і статистичних даних, міжнародних та українських нормативних актів у сфері кібербезпеки, і емпіричну перевірку на базі ретроспективного порівняльного аналізу ключових операційних метрик SOC у референтних інфраструктурах. Вибірка охоплювала періоди відносної стабільності та масових відключень електропостачання, що дозволило ідентифікувати кореляцію між зовнішніми чинниками середовища та деградацією показників ефективності.*

Наукова новизна. *У роботі системно ідентифіковано та структуровано специфічні виклики функціонуванню SOC в умовах сучасної повномасштабної війни: деградація енергетичної та телекомунікаційної інфраструктури, фізична окупація й втрата ІТ-активів, кадрова криза, кібервійна державного рівня та розрізненість нормативної бази. Продемонстровано вплив цих факторів для ключових метрик ефективності SOC.*

Висновки. *Ефективність підрозділу кібербезпеки в умовах повномасштабної війни визначається стійкістю до зовнішніх впливів та наявністю відповідних контролів. Практично це вимагає: резервування енергоживлення і зв'язку на критичних вузлах; буферизації телеметрії та відкладеної кореляції; заздалегідь опрацьованих сценаріїв ізоляції сегментів і ключів; гібридної організації праці із мінімізацією навантаження аналітиків; уніфікації контролів за «профілями безпеки» з прозорим відображенням на хмарні сервіси. Отримані результати задають пріоритети для розподілу ресурсів SOC і подальшого тестування контрзаходів.*

Ключові слова: *Security Operation Center, кібервійна, спостережність, окупація ІТ-активів, кадрова криза.*

Oleksandr POPOV, Roman DRAHUNTSOV. KEY CHALLENGES FOR SECURITY OPERATIONS CENTERS IN THE CONTEXT OF FULL-SCALE WAR

Abstract. *The article systematizes the key factors defining the effectiveness of commercial and governmental Security Operation Centers (SOC) in Ukraine during 2022–2025: degradation of energy and telecommunications infrastructure, occupation and physical loss of IT assets, state-level cyber warfare, workforce crisis, and transitional inconsistency of regulatory norms.*

Purpose. *To identify and assess the impact of environmental constraints on SOC operations under the conditions of a modern full-scale war, and to define the specific characteristics of cybersecurity threats in this context.*

Methodology. *The research combines a review of scientific and analytical sources and Ukrainian regulatory acts with a retrospective comparative analysis of SOC metrics across reference infrastructures.*

Scientific novelty. *The study identifies critical challenges specific to cybersecurity units operating in the context of full-scale warfare and evaluates their influence on SOC performance indicators.*

Conclusion. *The effectiveness of a cybersecurity unit under wartime conditions is determined by its resilience to external disruptions and the availability of appropriate controls. In practice, this requires: redundancy of power supply and communications at critical nodes; buffering of telemetry and deferred correlation; pre-defined scenarios for segment and key isolation; hybrid work organization with minimized analyst workload; and unification of control through "security profiles" with transparent mapping to cloud services. The obtained results define priorities for SOC resource allocation and further testing of countermeasures.*

Key words: *Security Operation Center, cyberwar, observability, occupation of IT-assets, staffing problems.*

Постановка проблеми. В умовах повномасштабної війни ландшафт кібербезпеки для України та світу суттєво змінюється. В період 2022–2025 рр. український кіберпростір став фактично одним із найбільш атакованих у світі – зокрема, у 2024 р. командою CERT-UA зафіксовано 4315 кібератак, що на 70 % перевищує показник попереднього року [1]. Близько 75 % усіх кібератак здійснених державними структурами російської федерації у 2022–2023 рр. були націлені саме на Україну [1]. Попри детальний розгляд проблематики кібервійни – від опису окремих кіберінцидентів до принципів ведення бойових дій в кіберпросторі – залишається менше висвітленою проблематика внутрішніх викликів забезпечення кібербезпеки: підтримка роботи операційних центрів кібербезпеки (тут і дали, Security Operation Center – SOC) комерційних компаній та державних установ в умовах кінетичних атак, відключень електропостачання, окупації територій та інших військових факторів. Актуальність дослідження зумовлена необхідністю ідентифікації конкретних проблем у функціонуванні SOC в умовах повномасштабної війни для визначення відповідних засобів для вирішення цієї проблематики, визначення методів розбудови SOC, що будуть ефективними з урахуванням реалій воєнного часу. Повномасштабні війни 21-го століття продемонстрували, що кіберскладова є надзвичайно важливим елементом національної обороноздатності [2], тому виявлення проблем та перешкод у функціонуванні SOC під час бойових дій є необхідним фактором забезпечення національної стійкості. В статті розглянуто ключові проблеми кібербезпеки, з якими стикнулися українські комерційні та державні SOC у період 2022–2025 рр.

Аналіз останніх досліджень та публікацій. У воєнний період питання кібербезпеки України висвітлюються у звітах, наукових дослідженнях та аналітичних оглядах: здебільшого відзначається кіберстійкість української держави, роль інноваційних рішень та залучення приватного сектору у протидії атакам, підкреслюється перехід після вторгнення 2022 р. від реактивної до проактивної моделі, інтегрованої у воєнну стратегію країни [3].

В розрізі проблематики розбудови SOC розглядається кадровий дефіцит, фрагментарність нормативної бази та недостатня координація між державним і приватним секторами у сфері кібербезпеки – відзначається необхідність інтеграції приватних та державних SOC у єдину інфраструктуру, підсилену автоматизацією, зокрема, на основі ШІ, задля зменшення часу реагування на інциденти [4]. В розглянутих роботах такі висновки зроблені на основі аналізу досвіду кібератак 2014–2023 рр. Оцінка кадрового дефіциту в домені кібербезпеки носить характер критичної проблеми в умовах воєнного стану [5, 6]. При цьому ж, дана тенденція також має і глобальний характер: глобальний розрив кадрів у сфері кібербезпеки сягнув 4 млн спеціалістів, а 59 % команд кібербезпеки у світі недоукомплектовані [6]. Криза в українських умовах посилюється змінами в структурі зайнятості і міграцією населення. Статистично ці факти відображаються в опитуванні Європейської Бізнес-Асоціації, які відображають, що 67 % українських компаній відчувають гострий дефіцит персоналу, дві третини роботодавців називають повномасштабну війну основною причиною даної проблеми.

Значна увага у літературі та наявних дослідженнях приділяється феномену кібервійни, який знаходиться поза рамок даного дослідження. Відзначається рекордний масштаб залучення Advanced Persistent Threat (APT-груп) державного рівня та кібер-криміналітету для досягнення військових цілей у кіберпросторі [1–7]. Російські хакерські угрупування використовують Україну як полігон для відпрацювання атак. Близько 75 % їхньої активності припадає на українські об'єкти, причому, схожі тактики та техніки застосовуються після цього глобально [1].

Існуюча література в основному не висвітлює впливів фізичного руйнування інфраструктури на функціонування підрозділів кібербезпеки, порушення доступності та нормального функціонування цивільної інфраструктури, зокрема, енергетичної та телекомунікаційної. Хоча дана проблематика є тісно пов'язаною з питаннями забезпечення життєстійкості критичної інфраструктури, специфіка даного питання розглядається лише в окремих дослідженнях [8]. Окрім питань нестачі персоналу внаслідок кадрової кризи обмежено розглядається питання географічного розподілення персоналу, необхідного часу адаптації кадрів та впливу морально-психологічного стану на ефективність роботи фахівців. В даній статті проводиться аналіз статистичних даних, що підтверджують кожен з факторів проблематики, визначається вплив на функціонування SOC під час повномасштабної війни.

Метою дослідження є визначення та оцінка впливу обмежень середовища на роботу SOC, визначення ключових особливостей загроз кібербезпеки в умовах сучасної повномасштабної війни для подальшого напрацювання методологій та підходів до розбудови SOC для приватних та державних підприємств у військовий час.

Виклад основного матеріалу дослідження. ***Руйнування енергетичної та телекомунікаційної інфраструктури.*** Фізичне знищення цивільної інфраструктури – одна з перших і найочевидніших проблем, з якими зіткнулися кібербезпекові підрозділи. Російські обстріли енергосистеми

спричинили масові та тривалі відключення електропостачання, що ускладнило роботу дата-центрів, мережевого обладнання, засобів моніторингу та створило навантаження на системи резервування. Внаслідок кінетичних атак на енергетику України наприкінці 2022 р. – на початку 2023 р. значна частина держави регулярно залишалася без електропостачання на періоди від декількох годин до декількох діб. Для забезпечення неперервності роботи SOC та IT-систем підприємства розгортають резервні джерела живлення і канали зв'язку, а також забезпечують моніторинг доступності. Як приклад, найбільший оператор телекомунікаційних послуг Kyivstar станом на 2024 р. розширив свою інфраструктуру резервування енергоживлення 2322 дизель-генераторами та понад 115 тисячами резервних батарей на базових станціях мобільного зв'язку по усій Україні [9]. Втрата електроживлення на значній частині території держави у розподілених IT-системах призводить до впливів на команди кібербезпеки у формі втрати каналів зв'язку для віддалених локацій інфраструктури та розривах у комунікації з сенсорами безпеки [10].

Для команд SOC пошкодження телекомунікаційної та енергетичної інфраструктури призводить до фрагментованості моніторингу. Відключення призводить до ізоляції окремих сегментів інфраструктури мережі на фізичному рівні, SOC втрачають видимість подій у цих сегментах. Аналіз інцидентів затримується, оскільки журнали подій недоступні в реальному часі, а сенсори (наприклад, мережеві Intrusion Detection System (IDS)) не мають зв'язку з центральними консолями керування. Зниження пропускної здатності мереж через аварійні схеми маршрутизації та супутникові канали призводить до збільшення часу реагування на інциденти. Ключовими контрзаходами є резервування енергоживлення критично важливих об'єктів на період визначений доцільним в рамках оцінки ризиків [11] та резервування каналів зв'язку за рахунок, зокрема, супутникових каналів [9]. Обов'язковим контрзаходом є впровадження детектуючих контролів безпеки для виявлення події зникнення електроживлення, вимкнення каналів зв'язку, зникнення зв'язності мережі. Також SOC повинен володіти знанням інфраструктури в розрізі динамічності та вразливості об'єктів до вимкнення електропостачання. Український досвід показав ефективність масового резервування джерел живлення, каналів зв'язку за рахунок супутникових терміналів, міграції сервісів у хмарні дата-центри та розподіл VPN-мереж. Порушення цілісності цивільної інфраструктури спричиняє низку проблем для SOC від фізичних перебоїв у роботі центрів обробки даних до деградації якості моніторингу та збільшення часу на реагування.

В рамках аналізу вибірки діючих SOC, досвід яких враховувався при написанні даної статті, було проаналізовано ключові ідентифікатори деградації параметрів роботи SOC в межах дії масових впливів відключення електропостачання, а саме: середній час реагування на інциденти до закриття (MTTR, Mean Time To Response), середній час ідентифікації інциденту (Mean Time To Detect) та середній відсоток доступності систем технологічної платформи SOC. Були розглянуті періоди грудень 2023 р. – лютий 2024 р. (Період 1, період відносної стабільності цивільної інфраструктури), червень – серпень 2024 р. (Період 2, період масових відключень електропостачання), грудень 2024 р. – лютий 2025 р. (Період 3, період відносної стабільності цивільної інфраструктури). Так, було відмічено збільшення MTTR в Період 2 у порівнянні з Періодом 1 на 24 % та в порівняння з Періодом 3 – на 26 %. Збільшення MTTD в Період 2 в порівнянні з Періодом 1 склало 425 %, в порівнянні з Періодом 3 – 412 %. Відсоток доступності ТП SOC для усіх інфраструктурних компонентів для Періоду 2 зменшився приблизно на 7 % в порівнянні з Періодами 1 та 3. Очевидна суттєва деградація ефективності виявлення інцидентів та інших показників кібербезпеки саме в період масових відключень електропостачання, що пояснюється саме кореляцією з періодами масових відключень електропостачання. Дана проблематика зумовлена саме аспектами середовища та доступності відповідних інфраструктурних сервісів, та, враховуючи взяття до уваги показників декількох різних SOC, менше стосується внутрішніх процесів окремих підрозділів кібербезпеки.

Окупація та втрата об'єктів IT-інфраструктури. Специфічною загрозою для кібербезпеки в рамках повномасштабної війни з динамічною лінією бойового зіткнення стає фактор окупації територій та об'єктів IT-інфраструктури. На відміну від кіберінцидентів мирного часу, коли об'єкти (дата-центри, вузли мережі, окремі кінцеві точки) переважно залишаються під фізичним контролем власників, під час війни певна частина IT-активів опиняється захопленою супротивником в непошкодженому стані або фізично знищується бойовими діями. Однією з загроз, які з'являються в даному сценарії, є захоплення фізичного контролю над фрагментом мережі для подальшого контролю та просування в мережевій інфраструктурі. Зокрема, російські сили на окупованих територіях України цілеспрямовано захоплювали вузли зв'язку та центри обробки даних з подальшим підключенням їх до російських мереж – подібна тактика фіксувалась у діях російських окупаційних військ починаючи з 2014 р. на території Донецької та Луганської областей та в Криму [7]. Після лютого 2022 р. ці ж методи застосовувалися і на новоокупованих територіях (Херсонщина, Запорізька область тощо), що призводило як до

інформаційної ізоляції окупованої території, так і до порушення цілісності мережевої інфраструктури не окупованої України. Протягом 2022 р. окупаційні війська здійснювали примусове переведення трафіку регіональних провайдерів через російські мережі (Khersontelecom – Miranda Media/Rostelecom, після первинного відключення і «переналаштування» каналів наприкінці травня 2022 р.), що фактично встановлювало цензуру та повний технічний контроль трафіку [7].

Окупація фізичних компонентів інфраструктури створює для SOC втрату видимості та системну кризу довіри: скомпрометованими вважаються всі канали зв'язку, ідентичності вузлів, журнали подій та засоби керування. Також регулярно може відбуватись часткове знищення або від'єднання обладнання українськими провайдерами, щоб не допустити його використання ворогом, та прискорене винесення державних реєстрів і критичних даних у хмарні середовища за межі регіонів ризику [12–15]. Модель загроз при окупації ІТ-активів представлено в (табл. 1).

Таблиця 1

Модель загроз при захопленні ІТ-активів

Загроза	Опис	Техніка Mitre Att&ck [16]
Компрометація мережевої маршрутизації	Примусовий BGP/AS-рерутинг через підконтрольні оператори створює стійкі умови для Adversary-in-the-Middle, DPI (Deep Packet Inspection), ін'єкції контенту та SSL-перехоплення, навіть без змін у кінцевих системах.	TA0001 Initial Access через T1557 Adversary-in-the-Middle
Фізичне втручання в обладнання	Доступ до фізичного майданчика дозволяє встановлювати інлайн-тапи, змінювати конфігурації L2/L3, підмінювати оптичні канали, переносити ключі з мережевих пристроїв, змінювати прошивки (ризики до рівня UEFI/Boot-ROM), активувати приховані облікові записи на BMC (iLO/iDRAC).	TA0001 Initial Access через T1557 Adversary-in-the-Middle
Викрадення секретів	Отримання супротивником доступу до резервних носіїв, вузлів з HSM, токенів доступу у системах, що можуть застосовуватись в іншій частині інфраструктури, конфігурацій, доступів до out-of-band (OOB).	TA0006 Credential Access – T1552 Credentials in Files TA0040 Impact – T1489 Service Stop/T1490 Inhibit System Recovery TA0008 Lateral Movement – T1021 Remote Services
Технічна деградація спостережності	Відключення або фальсифікація журналів, підміна NTP, ін'єкція фальшивих подій і телеметрії, перевидача сертифікатів підконтрольним CA (Certification Authority).	TA0005 Defense Evasion – T1562 Impair Defenses
Примусове «переведення» абонентів на окупаційні мережі	Розповсюдження SIM, що компрометує мережеві й телефонні канали.	TA0001 Initial Access через T1557 Adversary-in-the-Middle

Вплив на функціонування SOC спричиняє колапс домену довіри – усі активи в зоні окупації вважаються недовіреними незалежно від попередньої автентикації та MAC/IP, сертифікати, TPM чи стандартні IoC без постійного контролю фізичного стану локації втрачають необхідний рівень довіри. Дана проблема особливо актуальна в умовах динамічної лінії фронту російсько-української війни періоду лютого – червня 2022 р. Весь трафік у регіонах, в яких ведуться активні маневрені бойові дії, підлягає обробці за принципом treat-as-compromised. Також одним з найважливіших ризиків даної ситуації є ризик вторинної компрометації центру, тобто зміщення супротивника з окупованої частини ІТ-інфраструктури до центральної та довіреної частини. Site-to-site тунелі, SD-WAN мережі, об'єднанні системи аутентифікації, Single-Sign On, агенти моніторингу та реплікації резервних копій можуть стати шляхом зміщення супротивника всередину мережі.

Кадрова криза. Кадровий склад в умовах повномасштабної війни зазнає одного з найбільших негативних впливів. Українська ІТ-галузь і сфера кібербезпеки входили у повномасштабну війну у 2022 р. з певним кадровим дефіцитом, характерним для галузі у всьому світі, але військові дії суттєво загострили проблему. Зміна в структурі зайнятості населення, масова евакуація та еміграція фахівців за кордон, а також прямі втрати серед військовослужбовців-фахівців призвели до того, що багато центрів кібербезпеки втратили частину досвідчених співробітників. Станом на 2023–2024 рр. 67–74 % українських компаній повідомляли про нестачу кадрів зумовлену факторами повномасштабної війни. При цьому, статистично майже 60 % команд кібербезпеки у світі на момент 2025 р. недоукомплектовані [6]. Особливо відчутною є дефіцит висококваліфікованих кадрів (аналітиків рівня Senior, архітекторів безпеки тощо), пошук і підготовка яких потребують тривалого часу. Очевидно, що

для інших сучасних масштабних військових конфліктів проблематика впливу на доступність кадрового ресурсу буде актуальною [17].

Кадрова криза проявляється двома ключовими шляхами. Перший – прямий, тобто нестача спеціалістів для укомплектування команд SOC. На прикладі трьох референтних SOC було визначено проблематику хронічного дефіциту фахівців нічних змін та певний дефіцит фахівців другої лінії кіберзахисту. Середні показники комплектації команд відрізняються від довоєнних на 25 %. Другий аспект – розпорошення персоналу географічно. Через бойові дії значна частина IT-спеціалістів релокувалася у більш безпечні регіони держави або за кордон – статистично 20% українських IT-фахівців у 2023 р. працювали віддалено за межами України [18]. З урахуванням даних факторів суттєва частина SOC України переходять у віддалений або гібридний режими роботи, що є вимушеним та достатньо складним заходом з урахуванням специфічних вимог операційної безпеки. Окрім суто безпекової проблематики розподіленої роботи команд кібербезпеки є і операційна проблематика. Як вже розглядалось у одному з попередніх розділів, руйнування цивільної інфраструктури, такої як енергетична та телекомунікаційна, призводить до втрат зв'язку і розривів IT-систем. Для центрів обробки даних дана проблематика вирішується встановленням додаткових резервних джерел живлення та зв'язку, в той час як для індивідуальних фахівців подібні заходи вдома можуть бути недоступними – аналітик у віддаленому режимі може в будь-який момент втратити зв'язок з робочою інфраструктурою внаслідок зникнення електропостачання чи каналу зв'язку. Резервування на достатньому рівні робочих місць фахівців кібербезпеки в умовах віддаленої, розподіленої роботи неможливе в достатній мірі внаслідок їх високої вартості та необхідності великої кількості. В умовах відсутності зв'язку SOC залишається без відповідних фахівців, які, в свою чергу, можуть бути єдиними доступними на зміні на даний момент часу, зважаючи на проблему кадрової кризи. Другою проблемою є забезпечення безпеки доступу: забезпечення захищених каналів (Virtual Private Network – VPN, Virtual Desktop Infrastructure – VDI) для підключення співробітників з різних мереж зі збереженим рівнем довіри, що збільшує навантаження на IT-інфраструктуру [19].

Додатковою кадровою проблемою в розглянутих умовах є зниження оперативності обміну знаннями та навчання нових фахівців: У віддаленому режимі цей процес ускладнюється, також ускладнюється і питання введення в робочий режим нових співробітників. Навчання нових фахівців, знайомство їх з робочими процесами, колективом, ключовими принципами функціонування SOC у віддаленому режимі ускладнюється, збільшується тривалість – на прикладі розглянутих в дослідженні референсних SOC навчання та загальний онбордінг фахівців у повністю віддаленому режимі потребував в середньому на 7 % більше часу.

Ще один специфічний виклик кадрового характеру – психологічна стійкість і мотивація персоналу SOC. Робота аналітика кібербезпеки завжди містить високий рівень стресу, але під час військових дій рівень стресу співробітників суттєво зростає. До факторів стресу належать обстріли, зокрема й нічні, руйнування цивільної інфраструктури, острах за розвиток подій на фронті та близьких залучених до оборони, а також невизначеність майбутнього. Очевидно, що в умовах стресового та часто понаднормового реагування на інциденти рівень психологічної готовності команд кібербезпеки знижується, з ним знижується рівень мотивації та концентрації, що має очевидний вплив на ефективність виявлення та реагування на загрози. Впровадження ротацій фахівців, додаткових вихідних є дуже обмеженим за ефективністю заходом, однак фактичний вплив подібних підходів потребує додаткових досліджень. Очевидно, що надання додаткових вихідних в умовах кадрової кризи є не ефективним рішенням з огляду на хронічну нестачу персоналу.

Фактор кібервійни. Повномасштабне вторгнення російської федерації в Україну супроводжується інтенсивною кібервійною, у якій діє значна частина хакерських груп обох держав. З боку рф більшість таких загроз – це підрозділи спецслужб (так звані Advanced Persistent Threat, APT). Хоча кібератаки на українські держструктури відбувалися і раніше (з 2014 р. фіксувалися операції Sandworm, Armageddon/Gamaredon та інші), у 2022–2023 рр. їх масштаб зріс на порядки. З початку вторгнення лише державними регуляторами та незалежними компаніями з кібербезпеки зафіксовано кратне зростання кількості інцидентів різного рівня складності. Станом на 2025 р. Україна посідає 2-е місце у світі серед країн, що найбільше стикаються з кіберзлочинністю [1]. Для будь-якого SOC це означає істотне збільшення навантаження: обсяг інцидентів, що фіксуються SOC, та які потребують розслідування та реагування, зросла приблизно в 2,5 рази, що було визначено на прикладі референсних інфраструктур SOC.

Аналогічно до українського досвіду Ізраїль після початку активної фази війни з Хамас зазнав різкого збільшення тиску на інфраструктуру кіберзахисту. Після нападу Хамас 7 жовтня 2023 р. кількість звернень на гарячу лінію кібербезпеки державних кіберцентрів зросла в 10

разів – з близько 50 повідомлень до понад 500 на день, а число активних APT-груп, що атакували країну, подвоїлося [20]. Основними агентами загроз, що оперують у кібервійні проти Ізраїлю, є іранські державні структури та вільні угрупування, що корелює з українським досвідом.

Діяльність SOC ускладнюється комбінованими атаками, що синхронізуються з військовими діями: наприклад, 24 лютого 2022 р. паралельно з кінетичними обстрілами було виведено з ладу частину інфраструктури супутникової мережі ViaSat, атаковано інфраструктуру GigaTrans та на 15 год уражено частину мережі Укртелекому. Такі атаки здійснюються із застосуванням спеціалізованого шкідливого ПЗ (Industroyer2, CaddyWiper, Pterodo), а частка атак на критичну інфраструктуру України зросла з 20 % у 2021 р. до 40 % у 2022 р. Навантаження на функціонування SOC зростає і зумовлюється також фактором застосування супротивником постійно змінюваних та еволюціонуючих інструментів – майже кожен з використованих російськими APT-групами інструментів зазнає неперервного розвитку та еволюції. Це змушує команди SOC впроваджувати більше проактивних практик виявлення інцидентів, налагоджувати обмін розвідданими з розвідувальними джерелами та впроваджувати дані практики в операційні процеси. Очевидно, що успішне впровадження даних заходів потребує розширення виділених на функціонування SOC ресурсів, як людських так і фінансових, які є також значно обмеженими у військовий час.

Розрізненість нормативної бази. У березні 2022 р. Кабінет Міністрів України дозволив державним реєстрам та відповідним ІК-системам розміщуватися у хмарних/ЦОД (Центрах Обробки Даних) поза межами України на період дії воєнного стану з обов'язком припинити таке розміщення протягом шести місяців після його завершення. Це рішення легалізувало «цифрову евакуацію», але водночас поставило питання узгодженості з чинними галузевими та загальними вимогами захисту інформації. Паралельно держава формалізувала ринок хмар для публічного сектору: Закон України «Про хмарні послуги» [35] запровадив державний перелік провайдерів та регуляторний нагляд Держспецзв'язку. У 2025 р. регулятор актуалізував і деталізував порядок включення провайдерів до переліку, що створює основу для контрольованого використання хмар у державному секторі [21, 22] Системоутворюючими рамками стали також: Положення про організаційно-технічну модель кіберзахисту [23], загальні вимоги до кіберзахисту ОКІ (Об'єктів Критичної Інфраструктури) [26], Закон України «Про критичну інфраструктуру» (1882-IX, 2021 р.), Порядок реагування на події у кіберпросторі [30]. Сукупно вони задали «скелет» державної моделі кіберзахисту та координації реагування [23].

До 2024 р. основним операційним інструментом в державному регулюванні функціонування SOC були Нормативні Документи систем Технічного Захисту Інформації (НД ТЗІ) та атестація/експертиза Комплексних Систем Захисту Інформації (КСЗІ); у 2024–2025 рр. держава перейшла до ризик-орієнтованих «профілів безпеки» і запустила нову модель підтвердження відповідності: від експерименту з декларування [25] – до постійної моделі «авторизації з безпеки» та порядку профілювання [32]. Перехідний період спричинив накладання старих і нових процедур, різночитання щодо достатності контролів і дублювання оцінок [24; 25]. Загальнодержавні вимоги [23; 26; 30] співіснують із жорсткішими галузевими нормами, наприклад, Постанова НБУ № 95 [36], що веде до різних трактувань цільового рівня захисту, строків повідомлення про інциденти та змісту звітності. Для багатосекторних груп це породжує паралельні комплаєнс-процеси [26; 27]. Дозвіл Кабінету Міністрів України № 263 [33] на екстрене розміщення за кордоном змінив традиційну модель побудови КСЗІ, орієнтовану на національні процедури експертизи та локальне середовище. До появи оновлених профілів безпеки та порядку авторизації організаціям бракувало уніфікованих правил зіставлення «українських» вимог із практикою провайдерів Європейського Союзу, що ускладнювало підтвердження відповідності для гібридних/хмарних архітектур. Базовий Закон №2297-VI [28] залишається чинним (редакція 2025 р.), а оновлена редакція № 8153 [34], що гармонізує режим із GDPR (General Data Protection Regulation) (ухвалена у І читанні в листопаді 2024 р.), ще не набула чинності. Це створює невизначеність щодо підстав і гарантій транскордонної обробки даних, ролей контролера/процесора та санкційного режиму [28; 29].

Практично у функціонуванні SOC розрізненість нормативної бази має три ключові фактори впливу – задвоєння норм відповідності, нерівномірність процедур реагування та неоднозначності у трактовці вимог ризик-менеджменту на міждержавному рівні.

Організації, які одночасно є суб'єктами ОКІІ і піднаглядними галузевому регулятору, змушені підтримувати різні набори контролів, звітності та аудиторських процедур. Це підвищує операційні витрати та ризик виникнення явища формальної відповідності регуляторним вимогам [26; 27]. Загальний порядок реагування [30] і методичні рекомендації Держспецзв'язку задають єдину логіку етапів реагування на інциденти, але галузеві акти додають власні терміни та канали комунікації, що потребує узгоджених, багатовекторних планів оповіщення (CERT-UA, регулятор, клієнт) [30].

За умов розміщення даних/сервісів у ЄС вимагається явне відображення контролів НД ТЗІ/профілів безпеки на контрольні набори провайдерів і внутрішні політики провайдера, що є нетривіальною задачею [24; 28].

Проблематика розрізненості нормативної бази хоча і є актуальним викликом, натомість має тенденцію до вирішення протягом 2023–2025 рр. Зокрема, постановою КМУ № 712 [32] затверджено порядок розробки/затвердження профілів безпеки інформації та порядок авторизації з безпеки, Держспецзв'язку затвердив порядок моніторингу їх реалізації (наказ № 160, березень 2025 р.). Це уніфікує підходи до підтвердження відповідності й дозволяє будувати КСЗІ як ризик-орієнтовані конфігурації, сумісні з хмарними шаблонами [31]. НД ТЗІ зазнали оновлення – НД ТЗІ 3.6-006-24 і наказ Держспецзв'язку № 54 (січень 2025 р.) з «Базовими заходами» та методичними рекомендаціями фактично здійснюють відображення стандарту на сучасні домени [24]. Проблематика сприйняття хмарних інфраструктур в правовому полі вирішується в рамках закону № 2075-IX [35] – утворюються уніфіковані критерії допуску хмар до держсектору, що знижує правову невизначеність під час міграції інфраструктури [21, 22]. Прийняття нової редакції закону про персональні дані у другому читанні [34] має усунути недоліки регуляції транскордонності, прав суб'єктів та санкціях, що є важливим для хмарних операцій. У 2025 р. Національний банк України оновив Постанову № 95 [36], підвищивши вимоги до інформаційної безпеки у банківському секторі, Міністерство енергетики України готує секторальні вимоги до паливно-енергетичного комплексу з урахуванням державної моделі кіберзахисту. Таким чином, галузеві регуляторні вимоги наближуються до єдиного «ядра» контролів, що однозначно зменшує рівень розрізненості нормативної документації.

Висновки. Виконане дослідження показало, що на ефективність SOC в умовах сучасної повномасштабної війни впливає у значній мірі не лише внутрішня зрілість процесів, а й екзогенні обмеження середовища – насамперед деградація енергетичної й телекомунікаційної інфраструктури, втрата фізичного контролю над активами та зростання інтенсивності загроз. Емпіричні дані показали суттєве погіршення ключових метрик у періоди масових відключень електропостачання: приріст часу виявлення та реагування і зниження доступності технологічної платформи SOC.

Окремим важливим чинником виступає окупація й фізичне втручання в ІТ-активи, яке руйнує домен довіри й підвищує ймовірність вторинної компрометації через легітимні канали зв'язку. За цих умов раціональною стратегією є «treat-as-compromised» для прикордонних і близьких до лінії зіткнення сегментів, примусова сегментація та Zero Trust на міжсайтових з'єднаннях, попередньо авторизовані сценарії ізоляції, а також затримкостійкі ланцюги спостережності з буферизацією телеметрії та хмарними точками відновлення. Паралельно кадрова криза і географічне розпорошення персоналу зміщують оптимальну модель у бік гібридної організації праці з VDI/JIT-доступом, що потребує стандартизації онбордингу, підтримки психологічної стійкості та системного зменшення когнітивного навантаження для аналітиків.

Регуляторні зміни 2023–2025 рр. формують тренд до уніфікації вимог і ризик-орієнтованого підтвердження відповідності, однак перехідний період зберігає неоднозначність регуляторних вимог. Практичним наслідком для SOC є необхідність підтримувати «єдине ядро» контролів із чітким відображенням профілів безпеки на хмарні шаблони провайдерів і міжсекторально узгоджені процедури інцидент-менеджменту та звітності.

Життєздатний у сучасних воєнних умовах SOC – це ризик-орієнтована система, що поєднує мінімально необхідну спостережність за умов погіршеної видимості інфраструктури, превентивну сегментацію довіри, операційну автоматизацію та комплаєнс, гармонізований із хмарними архітектурами. Подальша робота ведеться над кількісною оцінкою ефективності контрзаходів під час блекаутів, верифікації метрик «мінімально життєздатної спостережності», порівняльному аналізі з іншими країнами, що діють в умовах кібервійни, а також на відстеженні впливу завершення регуляторного переходу на операційні витрати й якість реагування.

Список використаних джерел:

1. Microsoft Digital Defense Report 2024. URL: https://cdndynmedia1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf (дата звернення: 31.08.2025).

2. Cyber Digest. Огляд ключових подій у світі кібербезпеки за жовтень 2022. URL: https://www.rnbo.gov.ua/files/2022/NKCK/Cyber%20digest_Oct.pdf (дата звернення: 31.08.2025).

3. GMF – Ukraine's Cyber Defense: URL: https://www.gmfus.org/sites/default/files/2023-12/Kvartsiana%20-%20Ukraine%20Cyber%20-%20Report.pdf (дата звернення: 31.08.2025).

4. Prokopovych-Tkachenko D., Zvieriev V., Kozachenko I. Integration of Security Operations Centers (SOC) into Ukraine's national security system. *STATE SECURITY.* 2025. T. 1, № 5. С. 106–114. URL: https://doi.org/10.33405/2786-8613/2025/1/5/336736 (дата звернення: 01.09.2025).

5. Дефіцит кіберспеціалістів. Чому українські фахівці на вагу золота. URL: https://speka.media/deficit-kiberspecialistiv-comu-ukrayinski-faxivci-cinuyutsya-na-vagu-zolota-vzjr69 (дата звернення: 31.08.2025).

6. Ukraine's cyber specialists disrupt Russian industry backbone. URL: https://defence.nridigital.com/global_defence_technology_aug24/latest-news-ukraine_war_dominant_in_cyber_operations (дата звернення: 31.08.2025).

7. Локот Т. Russia's Networked Authoritarianism in Ukraine's Occupied Territories during the Full-Scale Invasion: Control and Resilience: URL: https://ppr.lse.ac.uk/articles/10.31389/lseppr.85 (дата звернення: 31.08.2025).

8. Drahuntsov R., Zubok V. Modeling of Cyber Threats Related To Massive Power Outages and Summary of Potential Countermeasures. Èlektronnoe *modelirovanie.* 2023. T. 45, № 3. С. 116–128. URL: https://doi.org/10.15407/emodel.45.03.116 (дата звернення: 01.09.2025).

9. Lipscombe P. Ukrainian telco Kyivstar to deploy more generators in fight against blackouts : URL: https://www.datacenterdynamics.com/en/news/ukrainian-telco-kyivstar-to-deploy-more-generators-in-fight-against-blackouts (дата звернення: 31.08.2025).

10. Зубок В. Ю., Драгунцов Р. І. Особливості розслідування та реагування на інциденти кібербезпеки в умовах масових відключень електропостачання. Матеріали V науково-практичної конференції «Безпека енергетики в епоху цифрової трансформації», м. Київ, 22 листопада 2023 р.

11. Драгунцов Р. І. Алгоритм управління ризиками кібербезпеки в умовах знищення енергетичної інфраструктури. Науково-практична конференція «Кібербезпека енергетики», м. Київ, 28 травня 2025 р.

12. Wired: Ukraine–Russia internet takeover: URL: https://www.wired.com/story/ukraine-russia-internet-takeover (дата звернення: 31.08.2025).

13. Russia descends iron curtain over occupied land, cuts people off in internet: URL: https://kyivindependent.com/russia-descends-iron-curtain-over-occupied-land-cuts-people-off-internet/ (дата звернення: 31.08.2025).

14. Safeguarding Ukraine's data to preserve its present and build its future (Amazon): URL: https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future (дата звернення: 31.08.2025).

15. One year of war in Ukraine (Cloudflare blog): URL: https://blog.cloudflare.com/one-year-of-war-in-ukraine/ (дата звернення: 31.08.2025).

16. MITRE ATT&CK : URL: https://attack.mitre.org/ (дата звернення: 31.08.2025).

17. Кадрова криза в Україні: брак спеціалістів: URL: https://www.rbc.ua/rus/news/kadrova-kriza-ukrayini-k-brak-spetsialistiv-1727103044.html (дата звернення: 31.08.2025).

18. Kyiv IT Market Review (EchoGlobal.tech): URL: https://echoglobal.tech/kyiv-it-market-review-industry-research/ (дата звернення: 31.08.2025).

19. How technology helped Ukraine resist during wartime (Microsoft news) : URL: https://news.microsoft.com/en-cee/2023/01/20/how-technology-helped-ukraine-resist-during-wartime/ (дата звернення: 31.08.2025).

20. Israel stage3 cyber wars with Iran proxies: URL: https://www.darkreading.com/threat-intelligence/israel-stage-3-cyber-wars-with-iran-proxies (дата звернення: 31.08.2025).

21. Пономаренко Н. Тимчасове розміщення державних реєстрів за кордоном: мета та строки дії: електронний ресурс. URL: https://eba.com.ua/tymchasove-rozmishhennya-derzhavnyh-reyestriv-za-kordonom-meta-ta-stroky-diyi (дата звернення: 31.08.2025).

22. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX: станом на 21 вересня 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 01.09.2025).

23. Про затвердження Положення про організаційно-технічну модель кіберзахисту: Постанова Кабінету Міністрів України від 29.12.2021 р. № 1426: станом на 26 грудня 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-п (дата звернення: 01.09.2025).

24. Нормативні документи системи ТЗІ : URL: https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi2024 (дата звернення: 31.08.2025).

25. Про реалізацію експериментального проекту з декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації: Постанова Кабінету Міністрів України від 30.05.2024 № 627: станом на 19 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/627-2024-п#Text (дата звернення: 01.09.2025).

26. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.2019 р. № 518: станом на 7 верес. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text (дата звернення: 01.09.2025).

27. Про затвердження Змін до деяких нормативно-правових актів Національного банку України з питань інформаційної безпеки та кіберзахисту: Постанова Національного Банку України від 25.02.2025 № 24.

28. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI: станом на 14 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 01.09.2025).

29. Про порядок денний тринадцятої сесії Верховної Ради України дев'ятого скликання: Постанова Верховної Ради України від 11.02.2025 р. № 4229-IX: станом на 21 серпня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/4229-20#Text (дата звернення: 01.09.2025).

30. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Постанова Кабінету Міністрів України від 04.04.2023 р. № 299. URL: https://zakon.rada.gov.ua/laws/show/299-2023-п#Text (дата звернення: 01.09.2025).

31. Про затвердження Порядку ведення Переліку надавачів хмарних послуг та/або послуг центру обробки даних та форми заяви про внесення надавача хмарних послуг та/або послуг центру обробки даних до Переліку надавачів хмарних послуг та/або послуг центру обробки даних: Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 07.04.2025 р. № 231. URL: https://zakon.rada.gov.ua/laws/show/z0778-25#Text (дата звернення: 01.09.2025).

32. Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем: Постанова Кабінету Міністрів України від 18.06.2025 р. № 712: станом на 19 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/712-2025-%D0%BF#Text (дата звернення: 01.09.2025).

33. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану: Постанова Кабінету Міністрів України від 12.03.2022 р. № 263: станом на 06 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/263-2022-%D0%BF#Text (дата звернення: 01.09.2025).

34. Про критичну інфраструктуру: Закон України від 25.10.2022 р. № 8153: станом на 21 вересня 2024 р. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/40707 (дата звернення: 01.09.2025).

35. Про хмарні послуги: Закон України від 28.06.2024 р. № 2075-IX: станом на 28 червня 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text (дата звернення: 01.09.2025).

36. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України: Постанова Національного Банку України від 28.09.2017 р. № 95: станом на 01 березня 2018 р. URL: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text (дата звернення: 01.09.2025).

Дата надходження статті: 18.09.2025
Дата прийняття статті: 20.10.2025
Опубліковано: 04.12.2025