УДК 351.861.3:004.056

Д. І. Прокопович-Ткаченко, В. П. Звєрєв, І. М. Козаченко

ІНТЕГРАЦІЯ ОПЕРАЦІЙНИХ ЦЕНТРІВ УПРАВЛІННЯ БЕЗПЕКОЮ (SOC) У СИСТЕМУ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Досліджено інтеграцію операційних центрів безпеки (Security Operations Centers, SOC) у систему національної безпеки України як ключового елемента захисту критичної інфраструктури та реагування на кіберзагрози. Розкрито роль таких центрів в умовах гібридної війни, дезінформації та цифрових атак. Проаналізовано також міжнародний досвід їх функціонування, зокрема у США, ЄС і НАТО, де використовуються автоматизовані системи, штучний інтелект і великі дані.

Визначено основні виклики для України: кадровий дефіцит, фрагментарність нормативної бази та недостатня координація між секторами. Запропоновано комплексний підхід до розвитку операційних центрів безпеки, що передбачає технологічну модернізацію, міжнародне співробітництво та посилену підготовку фахівців як основу для підвищення кіберстійкості держави.

Ключові слова: *операційні центри безпеки (SOC), кібербезпека, гібридна війна, кібератаки, інформаційна безпека, критична інфраструктура, моніторинг загроз, штучний інтелект, аналіз великих даних, міжнародне співробітництво, національна безпека.*

Постановка проблеми. У сучасних умовах динамічного розвитку інформаційних технологій і зростання кіберзагроз одним із пріоритетних завдань національної безпеки стає забезпечення кібербезпеки держави. Україна як держава, що зазнає систематичних кібератак (із боку державних і недержавних акторів), потребує ефективної системи виявлення, моніторингу та реагування на кіберінциденти. Операційні центри безпеки (Security Operations Centers, SOC) є ключовими елементами такої системи, оскільки забезпечують оперативне реагування на загрози, аналіз потенційних ризиків і координацію дій державних і приватних суб'єктів кібербезпеки.

Одна з головних проблем полягає у фрагментарності чинної системи кібербезпеки України, що зумовлено відсутністю єдиної стратегії інтеграції SOC у загальнодержавну безпекову інфраструктуру. Брак централізованого управління, ефективного обміну інформацією між державними і приватними структурами, а також недосконаліть нормативно-правової бази створюють значні виклики для ефективного функціонування SOC. Досвід провідних країн свідчить про доцільність побудови SOC на основі інноваційних технологій, зокрема штучного інтелекту, машинного навчання та поведінкового аналізу, що підвищують точність і швидкість реагування на загрози.

Водночас важливим напрямом розвитку є розширення міжнародної співпраці, насамперед із ЄС, НАТО та ENISA, для посилення координації у сфері кіберзахисту. Успішне функціонування SOC також неможливе без належного кадрового забезпечення: в Україні гостро бракує сертифікованих спеціалістів у цій сфері. Тому у статті проаналізовано сучасні підходи до підготовки кадрів, зокрема впровадження міжнародних сертифікаційних програм та освітніх ініціатив.

З огляду на зростання кількості та складності кібератак інтеграція SOC у систему національної безпеки України є критично важливою. Розв'язання цієї проблеми потребує комплексного підходу, що охоплює технологічну модернізацію, розвиток нормативно-правової бази, кадрове зміцнення і міжнародну координацію. Такий підхід сприятиме посиленню кіберстійкості держави та ефективному захисту критичних інформаційних систем.

Аналіз останніх досліджень і публікацій. Проблематика інтеграції операційних центрів безпеки у систему національної безпеки України активно досліджується у науковій літературі. Найбільш розвинені SOC діють у США, ЄС і НАТО, де впроваджено стандартизовані підходи до моніторингу загроз, автоматизовані системи реагування та ефективну координацію між державним і приватним секторами [3, 6]. У доповідях European Union Agency for Network and Information Security (ENISA) та Cooperative Cyber Defence Centre of Excellence (CCDCOE) акцентується на важливості централізованого управління SOC для забезпечення оперативного реагування [3]. В Україні питання SOC досліджуються Computer Emergency Response Team of Ukraine (CERT-UA) та Національним координаційним центром кібербезпеки (НКЦК), які аналізують кібератаки 2014–2024 рр. Вбачається необхідність інтеграції SOC у загальнодержавну систему кібербезпеки [2]. У науковій праці [8] автори звертають увагу на недостатнє фінансування, кадровий дефіцит і необхідність оновлення нормативно-правової бази [9]. Окремо розглядаються технологічні аспекти SOC, зокрема впровадження штучного

інтелекту та машинного навчання для аналізу загроз [5, 6]. Автоматизація процесів дає змогу підвищити ефективність реагування і мінімізувати людський фактор. Критично бракує кваліфікованих кадрів, такий стан потребує запровадження освітніх програм і міжнародної сертифікації фахівців [10, 12].

Отже, останні дослідження підтверджують необхідність комплексного підходу до інтеграції SOC, що охоплює вдосконалення законодавства, розвиток технологій, підготовку кадрів та міжнародну співпрацю [3, 6].

Метою статті є дослідження ролі оперативних центрів безпеки (SOC) у системі національної кібербезпеки України, аналіз міжнародного досвіду їх упровадження, викликів для України, а також перспектив розвитку з урахуванням новітніх технологій, міжнародної співпраці та кадрового забезпечення.

Виклад основного матеріалу. У дослідженні застосовано комплексний методологічний підхід, що поєднує кілька наукових методів аналізу для забезпечення всебічного дослідження функціонування операційних центрів безпеки (SOC) в Україні. Метод порівняльного аналізу використано для зіставлення особливостей функціонування SOC в Україні з практиками, прийнятими у міжнародному середовищі, зокрема у США та країнах Європейського Союзу [2]. Це дає змогу виявити ключові відмінності у підходах до організації SOC, рівні їхньої інтеграції у державні системи кібербезпеки, застосуванні автоматизованих технологій та рівні співпраці з приватним сектором [4].

Аналіз міжнародного досвіду вкрай важливий для розроблення рекомендацій з удосконалення SOC в Україні та гармонізації їх діяльності з європейськими і світовими стандартами [7]. Метод аналізу даних застосовано для систематизації та оброблення інформації щодо кіберінцидентів, зафіксованих в Україні протягом 2014–2024 рр. [6]. До досліджуваних параметрів належать статистичні дані про кількість і види атак, джерела загроз, характер уразливостей, що використовували зловмисники, а також заходи реагування, упроваджувані SOC [9]. Цей метод дає змогу виявити закономірності в розвитку кіберзагроз, оцінити ефективність роботи SOC у різні періоди, а також ідентифікувати ключові напрями вдосконалення кіберзахисної інфраструктури [10].

Метод структурного аналізу використано для визначення організаційної структури SOC, їхніх функціональних можливостей, а також механізмів взаємодії з державними і приватними установами, що забезпечують кібербезпеку в Україні [3]. Зокрема аналізуються такі аспекти, як управління подіями інформаційної безпеки, виявлення загроз, реагування на інциденти, моніторинг трафіку, а також взаємодія SOC з органами державної влади, Національним координаційним центром кібербезпеки (НКЦК), CERT-UA та міжнародними партнерами [8]. Дослідження структури SOC дає змогу оцінити їхню оперативну ефективність, ступінь інтеграції у національну систему кіберзахисту та можливості щодо адаптації до нових викликів [12].

Метод прогнозування застосовано до оцінювання потенційних напрямів розвитку SOC в Україні, зокрема впровадження інноваційних технологій у сферу кібербезпеки [5]. Особлива увага приділяється перспективам використання штучного інтелекту, нейромережевих алгоритмів та цифрових двійників для вдосконалення процесів моніторингу, аналізу й реагування на кіберзагрози [13]. Прогностичний аналіз також уможливлює оцінювання довгострокових ризиків для кібербезпеки України, зокрема постквантові загрози, які можуть виникати внаслідок розвитку квантових обчислень, і розроблення рекомендацій щодо адаптації SOC до майбутніх технологічних змін [14].

Метод експертного аналізу використано для оцінювання ефективності роботи SOC, ідентифікації основних проблем та розроблення стратегічних заходів для вдосконалення їх діяльності [11]. Вивчалися думки експертів у сфері кібербезпеки, представників державних установ, аналітичних центрів та приватних компаній, які працюють у сфері інформаційної безпеки [15]. Аналіз експертних оцінок дає змогу зробити висновки щодо відповідності поточних підходів міжнародним стандартам, оцінити ступінь готовності SOC до реагування на сучасні загрози й визначити першочергові кроки для їх розвитку [18].

Отже, застосування зазначених методів створює комплексне уявлення про стан SOC в Україні, їхню роль у системі національної кібербезпеки, а також дає змогу визначити основні виклики й перспективи розвитку в контексті глобальних тенденцій у сфері кіберзахисту [20].

Задля підтвердження значущості SOC у системі кібербезпеки України варто звернутися до прикладів успішного виявлення та нейтралізації масштабних кібератак протягом останнього десятиліття. SOC відіграли ключову роль у відновленні роботи критичних систем, ізоляції заражених середовищ та реалізації протидій у режимі реального часу. У таблиці 1 подано хронологію найпоказовіших кіберінцидентів, що стали викликом для державних і приватних суб'єктів, а також охарактеризовано відповідні дії з боку оперативних центрів безпеки.

Таблиця 1 – Приклади атак, нейтралізованих в Україні із застосуванням SOC (2014–2024 рр.)

Рік	Подія	Опис	Джерело
2014	Атака на Центральну виборчу комісію України	Масштабна кібератака на сервери ЦВК, спрямована на зрив виборчого процесу. Відновлено роботу системи завдяки SOC та CERT-UA	[2]
2015	Атака на енергетичну інфраструктуру (BlackEnergy)	Кібератака на енергетичну систему України, що спричинила відключення електроенергії. Ідентифіковано ПЗ BlackEnergy	[2]
2017	Атака вірусу NotPetya	Масована кібератака вірусу NotPetya, що вразила державні установи та приватний сектор. Уражені системи ізольовано	[1]
2021	Кампанія WhisperGate	Виявлено шкідливу кампанію WhisperGate, спрямовану на дестабілізацію урядових систем. Ужито заходів захисту	[2]
2022	DDoS-атаки на платформи «Дія» та державні сервіси	SOC нейтралізували численні DDoS-атаки на портали «Дія» та урядові сервіси	[2]
2024	Постійне вдосконалення SOC	Удосконалення SOC, упровадження автоматизованих технологій, співпраця з такими міжнародними партнерами, як ENISA	[3]

Під час атаки 2014 р. на сервери Центральної виборчої комісії SOC у координації із CERT-UA нейтралізувано шкідливе ПЗ, яке могло дестабілізувати виборчий процес [2]. У 2015 р. під час атаки BlackEnergy на енергетичну інфраструктуру SOC ідентифіковано шкідливе програмне забезпечення та розроблено заходи з відновлення енергетичних систем [2]. У 2017 р. атака вірусу NotPetya продемонструвала здатність SOC оперативно реагувати на масові інциденти, ізолюючи уражені системи і зменшуючи масштаби катастрофи [1, 3]. Після початку повномасштабного вторгнення у 2022 р. SOC, використовуючи сучасні автоматизовані технології для захисту національного кіберпростору, активно блокували DDoS-атаки на державні сервіси, зокрема платформу «Дія» [2, 3].

Завдяки зазначеним функціям SOC стали невід'ємним складником національної системи кібербезпеки України, сприяючи захисту критичної інфраструктури від дедалі більшої кількості та зростаючої складності атак. Операційні центри безпеки демонструють ефективність не лише у виявленні загроз, але й у зміцненні інформаційного простору, що є стратегічним чинником у протидії гібридним війнам.

Інтеграція SOC у національну безпекову інфраструктуру є ключовим завданням для забезпечення ефективного захисту держави від сучасних кіберзагроз. Цей процес потребує тісної координації між такими державними органами, як CERT-UA, Служба безпеки України, Міністерство цифрової трансформації, і приватними структурами, що займаються інформаційною безпекою. Головними елементами такої інтеграції є обмін даними про кіберзагрози, уніфікація стандартів реагування на інциденти та стандартизація процесів аналізу й управління ризиками [1, 2].

Для підвищення рівня інформаційної безпеки України необхідно розглядати SOC не лише у практичному аспекті, але й інтегрувати наукові і технологічні підходи до їх розвитку. Використання інноваційних адаптивних моделей, побудованих на основі нейромереж, дасть змогу забезпечити більш точне виявлення кіберзагроз у реальному часі. Такі моделі здатні самонавчатися, аналізуючи масиви даних із минулих атак, і прогнозувати нові вектори загроз із високим рівнем точності. Так, упровадження технології цифрових двійників для симуляції роботи SOC може стати ефективним інструментом для моделювання й аналізу потенційних сценаріїв атак, а також для відпрацювання методів реагування у контрольованому середовищі [3].

Цифрові двійники дають змогу створювати точні віртуальні копії систем кібербезпеки, які можна використовувати для тестування нових методів захисту без ризику для реальної інфраструктури. У поєднанні з нейропрогностичними алгоритмами ці технології надають можливість прогнозувати ймовірні атаки й реагувати на них до того, як ті завдаватимуть шкоди. Наприклад, нейромережі здатні аналізувати трафік мережі, виявляти аномалії та автоматично активувати механізми захисту до моменту, поки атака набуде критичного масштабу [3].

Крім того, інтеграція SOC у глобальну систему безпеки передбачає активну співпрацю з такими міжнародними організаціями, як ENISA, для обміну найкращими практиками і використання передових рішень у сфері кібербезпеки. Це дає змогу гармонізувати національні підходи із загальносвітовими і забезпечити вищий рівень кіберзахисту держави [3].

Схема на рисунку 2 ілюструє основні функції операційного центру безпеки (SOC), які є ключовими для забезпечення кібербезпеки організації. Провідним є центр, який виконує координаційну роль у таких завданнях: управління подіями та інцидентами; аналіз інформаційної безпеки; управління вразливостями; захист веб-додатків; захист від кіберзагроз, DDoS-атак; збереження бренду. Крім того, він відповідає за експлуатацію засобів захисту, забезпечуючи цілісність, доступність і конфіденційність інформаційних активів. Схема наочно демонструє комплексний підхід до управління ризиками, який базується на взаємодії технологічних, процесних та аналітичних компонентів.

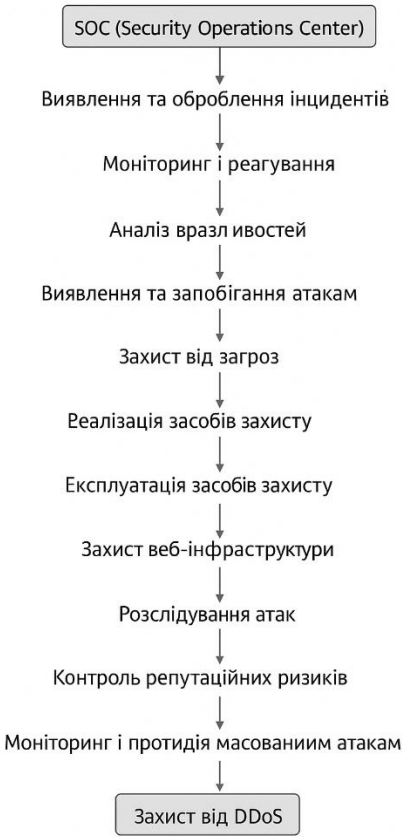

Рисунок 2 – Функціональна структура операційного центру безпеки (SOC)

Схема відображає ключові функції операційного центру безпеки SOC), які забезпечують комплексний підхід до кіберзахисту організації. SOC становить центральний вузол, який координує різні аспекти інформаційної безпеки і виконує низку важливих завдань. Експлуатація засобів захисту передбачає правильне налаштування, моніторинг і підтримку таких систем безпеки, як міжмережеві екрани, антивірусні програми та системи виявлення вторгнень. Управління подіями та інцидентами інформаційної безпеки передбачає моніторинг мережевого трафіку, виявлення аномалій, аналіз інцидентів і оперативне реагування на загрози для мінімізації їхнього впливу на бізнес-процеси. Управління вразливостями спрямоване на ідентифікацію та усунення слабких місць у програмному забезпеченні, системах і мережах для запобігання потенційним атакам. Захист веб-додатків забезпечує їхню безпеку від атак, зокрема SQL-ін’єкцій, міжсайтового скриптингу (XSS) та інших видів шкідливої

активності. Аналіз інформаційної безпеки охоплює збирання, оброблення та аналіз даних про кіберзагрози з метою розроблення стратегій захисту й запобігання майбутнім атакам. Захист від DDoS-атак передбачає запобігання розподіленим атакам типу «відмова в обслуговуванні», спрямованим на перевантаження систем і порушення їхньої роботи. Захист бренду передбачає моніторинг інформаційного простору для виявлення загроз репутації, пов'язаних із витоками даних, фішинговими атаками або незаконним використанням бренду. Захист від кіберзагроз та атак забезпечує цілісність, конфіденційність і доступність даних, а також протидіє таким сучасним загрозам, як фішинг, віруси та шкідливі програми.

Наведена схема демонструє багатокомпонентну природу SOC, який поєднує технологічні інструменти, аналітику і процеси для створення інтегрованої системи кіберзахисту. SOC виконує не лише реактивну функцію реагування на загрози, а й проактивну роль у запобіганні їм та мінімізації впливу на інформаційну інфраструктуру.

Реалізація інтеграції SOC у систему національної безпеки України вимагає комплексного підходу, що передбачає впровадження сучасних технологій, створення ефективної платформи обміну даними та розвиток кадрового потенціалу. Одним із ключових аспектів є використання технологій автоматизації для моніторингу й реагування на кіберзагрози. Упровадження штучного інтелекту, машинного навчання та нейропрогностичних алгоритмів дає змогу значно скоротити час реакції на інциденти і підвищити точність аналізу загроз. Однак для забезпечення довгострокової ефективності SOC необхідно враховувати майбутні виклики, зокрема постквантові загрози, які можуть зробити традиційні криптографічні алгоритми вразливими. Реалізація криптографічних рішень, стійких до атак із використанням квантових комп'ютерів, сприятиме захисту інформаційної інфраструктури від потенційних ризиків майбутнього.

Важливим компонентом інтеграції SOC є створення централізованої платформи для обміну інформацією про кіберзагрози між державними структурами, приватним сектором і міжнародними партнерами. Така система має забезпечувати швидкий аналіз даних, координацію дій і спільне реагування на інциденти в режимі реального часу. Використання технологій аналізу великих даних і штучного інтелекту сприятиме підвищенню ефективності роботи SOC і поліпшенню загального рівня кібербезпеки.

Важливим викликом є також і дефіцит кваліфікованих фахівців у сфері кібербезпеки, що обмежує спроможність SOC ефективно функціонувати. Вирішення цього питання передбачає розроблення спеціалізованих навчальних програм, упровадження систем сертифікації фахівців, а також створення умов для підвищення кваліфікації діючого персоналу. Важливу роль у цьому процесі відіграє міждисциплінарний підхід, що охоплює навчання адаптивним методам захисту, здатним ефективно реагувати на складні й динамічні загрози. У результаті реалізації цих заходів SOC в Україні можуть стати не лише елементом реагування на кіберзагрози, але й інтегрованою самоорганізованою системою, що використовує адаптивні алгоритми для забезпечення стійкості інформаційної інфраструктури держави. Це дасть змогу ефективно протидіяти сучасним і майбутнім загрозам, зміцнюючи національну безпеку в умовах цифрової трансформації.

Таблиця 2 – Основні напрями реалізації інтеграції SOC у систему національної безпеки

Напрям реалізації	**Основні заходи**	**Очікувані результати**
Автоматизація SOC	Упровадження штучного інтелекту, машинного навчання, криптографічних рішень, стійких до квантових атак	Підвищення точності та швидкості реагування на загрози, зменшення ризиків
Інтеграція платформи обміну даними	Створення централізованої системи обміну інформацією, застосування великих даних для аналізу загроз	Краща координація між державними і приватними структурами, ефективніша боротьба з кіберзагрозами
Підготовка кадрів у сфері кібербезпеки	Розроблення навчальних програм, сертифікація фахівців, підвищення кваліфікації персоналу	Збільшення кількості кваліфікованих фахівців, зменшення відтоку кадрів за кордон

Задля забезпечення ефективної інтеграції SOC у систему національної безпеки України необхідно приділити увагу розробленню нормативно-правової бази, яка б чітко визначала роль, функції та повноваження SOC, а також механізми їхньої взаємодії з іншими суб'єктами кібербезпеки. Це передбачає створення законодавчих актів і нормативних документів, що регулюють обмін інформацією про кіберінциденти, стандартизацію процедур реагування на загрози та забезпечення правових підстав для діяльності SOC.

Крім того, важливим аспектом є підвищення рівня обізнаності суспільства щодо кіберзагроз і ролі SOC у їх нейтралізації. Доцільним вбачається проведення інформаційних кампаній, навчальних програм і тренінгів для різних категорій населення, а також сприяння розвитку культури кібербезпеки в організаціях та установах. Забезпечення належної обізнаності й підготовки кадрів сприятиме ефективнішому використанню можливостей SOC і підвищенню загального рівня кіберстійкості держави.

Висновки

Інтеграція операційних центрів безпеки (SOC) у систему національної безпеки України є стратегічним завданням, що забезпечує захист критичної інфраструктури і зміцнює стійкість держави до сучасних кіберзагроз. Проведений аналіз засвідчив, що SOC виконують ключову функцію у виявленні, моніторингу, аналізі та нейтралізації кібератак, а їх ефективність безпосередньо залежить від рівня технологічного розвитку, кадрового потенціалу та рівня координації між державними і приватними структурами.

Незважаючи на досягнення у функціонуванні SOC, залишаються актуальними проблеми фрагментованості інфраструктури, браку кваліфікованих фахівців і обмеженого фінансування. Виклики гібридної війни, спрямовані атаки на критичні об'єкти, розвиток квантових технологій вимагають упровадження нових стратегій. Одним із провідних напрямів модернізації є інтеграція принципів синергетики, які сприяють створенню адаптивних і самоорганізованих систем. Використання штучного інтелекту, машинного навчання, цифрових двійників та прогнозних алгоритмів дає змогу підвищити швидкість і точність реагування на приховані і складні загрози.

У цьому контексті особливого значення набуває розвиток постквантових криптографічних рішень, які мають забезпечити довготривалий захист інформаційних систем. Водночас актуальним залишається питання підготовки кадрів: упровадження міждисциплінарних програм, сертифікацій і державної підтримки сприятиме формуванню професійного кадрового резерву у сфері кіберзахисту. Крім того, важливо враховувати міжнародний досвід, зокрема стандартизовані протоколи реагування, централізовані системи обміну інформацією та активну міждержавну співпрацю.

Напрямами подальшого дослідження вбачаються формалізація моделі інтегрованого SOC з урахуванням українського контексту, розроблення алгоритмів автоматизованого управління інцидентами, адаптація постквантових криптографічних рішень до реальних умов, а також вивчення ефективності міжсекторальної координації у системі національної кібербезпеки. Перспективним є також аналіз нормативно-правових механізмів для розбудови національної системи SOC з участю приватного сектору і міжнародних партнерів.

Перелік джерел посилання

1. Повідомлення про вірус NotPetya: аналіз і заходи реагування. Київ : CERT-UA, 2017. URL: https://cert.gov.ua (дата звернення: 08.02.2025).

2. Кіберзахист урядових систем під час військових дій. Київ : CERT-UA, 2022. URL: https://cert.gov.ua (дата звернення: 08.02.2025).

3. Cybersecurity Guide for SOCs. Athens : ENISA, 2021. URL: https://www.enisa.europa.eu (дата звернення: 08.02.2025).

4. Кіберзахист критичної інфраструктури: підходи до реагування. Київ : CERT-UA, 2020. URL: https://cert.gov.ua (дата звернення: 08.02.2025).

5. «Про національну безпеку України» : Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 08.02.2025).

6. National Cybersecurity and Communications Integration Center (NCICC). URL: https://www.cisa.gov (дата звернення: 08.02.2025).

7. Сопілко І. М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Юридичний вісник. Повітряне і космічне право*. 2021. Вип. 59. С. 110–115. DOI: 10.18372/2307-9061.59.15603.

8. Бєлкін Л., Юринець Ю., Бєлкін М., Криволап Є. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020–2021 років. *Юридичний вісник. Повітряне і космічне право*. 2022. Т. 3. Вип. 64. С. 78–86. DOI: 10.18372/2307-9061.64.16893.

9. Булашенко А. В., Бруй М. Інформаційна безпека. Суми : СумДУ, 2010. URL: http://essuir.sumdu.edu.ua/handle/123456789/21090 (дата звернення: 08.02.2025).

10. Кісілевич-Чорнойван О. М. Інформаційна безпека та міжнародна інформаційна безпека: проблема визначення понять. *Юриспруденція: теорія і практика.* 2009. № 8 (58). С. 11–18.

11. Суббот А. Інформаційна безпека суспільства. *Віче.* 2015. № 8 (388). С. 29–31.

12. Батечко О., Цимбаленко Н. В. Інформаційна безпека підприємства. Київ : Київський національний університет технологій та дизайну, 2016. URL: https://er.knutd.edu.ua/handle/123456789/4464 (дата звернення: 08.02.2025).

13. Захаров Є. Інформаційна безпека: що захищаємо? *Свобода висловлювань і приватність*. 2013. № 4. С. 3–6.

14. Шопіна І. М. Інформаційна безпека цифрової трансформації. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична).* Львів : ЛДУ ВС, 2023. Вип. 1. С. 28–35. DOI: 10.32782/2311-8040/2023-1-4.

15. Лосев І. Інформаційна безпека: як укріпити. *День*. 2014. № 82/83. С. 19.

16. Потапенко О. К. Державна інформаційна політика та безпека. *Вісник Київського національного університету імені Тараса Шевченка. Філософія. Політологія.* Київ : КНУ імені Тараса Шевченка, 2011. Вип. 102. С. 48–51.

17. Нестеренко О. Свобода інформації чи інформаційна безпека? *Свобода висловлювань і приватність*. 2011. № 1. С. 3–9.

18. Соловій Г. Р. Міжнародна інформаційна безпека: польський досвід. *Актуальні проблеми міжнародних відносин.* 2006. Вип. 65. С. 45–47.

19. Гуцалюк М. Інформаційна безпека у сучасному суспільстві. *Право України.* 2005. № 7. С. 71–74.

20. Глушков В. Інформаційна безпека (соціально-правові аспекти). *Право України.* 2010. № 9. С. 311–313.

21. Маракова І. І., Сиропятов О. А. Інформаційна безпека комплексних систем зв'язку. *Ukrainian Information Security Research Journal*. 2006. Т. 8. Вип. 4 (31). DOI: 10.18372/2410-7840.8.4977.

Стаття надійшла до редакції 15.04.2025 р.

UDC 351.861.3:004.056

D. Prokopovych-Tkachenko, V. Zvieriev, I. Kozachenko

INTEGRATION OF SECURITY OPERATIONS CENTERS (SOC) INTO UKRAINE'S NATIONAL SECURITY SYSTEM

The article explores the integration of Security Operations Centers (SOC) into Ukraine's national security system, emphasizing their role in strengthening cybersecurity resilience and protecting critical infrastructure. Given the increasing number of cyberattacks targeting Ukraine, SOCs serve as key components in detecting, monitoring, and responding to threats in cyberspace. The study analyzes the global experience of SOC implementation, particularly in the USA, EU, and NATO, where automated threat analysis systems, artificial intelligence, and big data analytics are widely employed to enhance cybersecurity operations [3, 6]. A significant part of the study is devoted to the challenges Ukraine faces in implementing SOCs, including insufficient funding, a shortage of qualified cybersecurity specialists, outdated legislation, and the need for integration with existing cybersecurity mechanisms [2, 4]. The article identifies key directions for SOC development in Ukraine, including the adoption of AI-driven cybersecurity technologies, expansion of

international cooperation, and improvements in specialist training programs [5, 8]. The research also highlights the need for a comprehensive approach to SOC integration, focusing on centralized coordination between state institutions, private sector actors, and international cybersecurity organizations such as ENISA and CERT-UA. The authors emphasize the importance of implementing automated threat detection and response systems, developing machine learning models for cyber threat intelligence, and enhancing international collaboration in cybersecurity policymaking [3, 6].

Keywords: *security operations center (SOC), cybersecurity, national security, hybrid warfare, cyber attacks, critical infrastructure protection, threat monitoring, artificial intelligence, big data analysis, incident response, international cooperation.*

ПРОКОПОВИЧ-ТКАЧЕНКО Дмитро Ігорович – кандидат технічних наук, доцент, завідувач кафедри кібербезпеки, Університет митної справи та фінансів
https://orcid.org/0000-0002-6590-3898

ЗВЄРЄВ Володимир Павлович – кандидат технічних наук, старший науковий співробітник, доцент кафедри інженерії програмного забезпечення та кібербезпеки. Державний торговельно-економічний університет
https://orcid.org/0000-0002-0907-0705

КОЗАЧЕНКО Ігор Миколайович – начальник підрозділу Державного центру кіберзахисту. Державна служба спеціального зв'язку та захисту інформації України
https://orcid.org/0000-0002-0774-7284