УДК 343.9:004.056:351.746.1
DOI https://doi.org/10.24144/2788-6018.2026.02.2.67

ЗАПОБІГАННЯ КІБЕРАТАКАМ ІНОЗЕМНИХ СПЕЦСЛУЖБ НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Погорецький М.М.,
доктор юридичних наук, старший дослідник,
доцент кафедри кримінального права та кримінології,
Навчально-науковий гуманітарний інститут
Національної академії СБ України
ORCID: 0000-0003-2888-0911
e-mail: pognikolay@gmail.com

Клименко С.В.,
кандидат юридичних наук, доцент,
завідувач кафедри кримінального права та кримінології,
Навчально-науковий гуманітарний інститут
Національної академії СБ України
ORCID: 0009-0004-2629-2133
e-mail: serklymenko@gmail.com

Погорецький М.М., Клименко С.В. Запобігання кібератакам іноземних спецслужб на об'єкти критичної інформаційної інфраструктури України.

У статті досліджено теоретичні та прикладні аспекти запобігання кібератакам іноземних спеціальних служб на об'єкти критичної інформаційної інфраструктури України в умовах триваючої збройної агресії. Обґрунтовано, що сучасні кібератаки на ОКІІ мають комплексну природу та виступають не лише технічними інцидентами, а й складовою розвідувально-підривної діяльності іноземних держав у кіберпросторі. Визначено, що ефективна протидія таким загрозам потребує поєднання технічних засобів кіберзахисту та контррозвідувальних механізмів, спрямованих на попередження, виявлення, документування та нейтралізацію джерел кіберзагроз.

Проаналізовано діяльність APT-угруповань, пов'язаних зі спеціальними службами іноземних держав, а також розкрито їхню роль у реалізації стратегічних кібероперацій проти України. Здійснено компаративний аналіз моделей захисту ОКІІ у США, Держави Ізраїль та Республіки Естонія, що дозволило встановити ключову системоутворювальну роль розвідувальних і контррозвідувальних органів у забезпеченні кібербезпеки. Доведено, що ефективні національні моделі базуються на інституціоналізованому обміні розвідувальною інформацією, публічно-приватному партнерстві та інтеграції цивільних, військових і розвідувальних спроможностей.

Проаналізовано чинну нормативно-правову базу України у сфері захисту ОКІІ та виявлено її ключові недоліки, зокрема відсутність належної інституційної інтеграції контррозвідувальної діяльності до системи кіберзахисту, недостатню ефективність механізмів обов'язкового повідомлення про кіберінциденти та відсутність нормативно закріпленого кіберрезерву. Запропоновано напрями вдосконалення законодавства, що передбачають запровадження механізмів обов'язкового обміну розвідувальною інформацією, посилення контррозвідувальних повноважень у сфері захисту ОКІІ, формування кіберрезерву та розвиток правових засад атрибуції кібератак. Зроблено висновок про необхідність переходу від реактивної до проактивної моделі контррозвідувального забезпечення кібербезпеки України.

Отримані результати мають практичне значення для вдосконалення державної політики у сфері захисту об'єктів критичної інформаційної інфраструктури та підвищення ефективності діяльності суб'єктів національної системи кібербезпеки України.

Ключові слова: кібербезпека; об'єкти критичної інформаційної інфраструктури; кібератаки; контррозвідувальна діяльність; іноземні спеціальні служби; кіберзлочинність; кібертероризм; національна безпека; детермінанти; запобігання.

Pohoretskyi M.M., Klymenko S.V. Preventing cyberattacks by foreign intelligence services against Ukraine's critical information infrastructure.

The article examines theoretical and applied aspects of preventing cyberattacks conducted by foreign intelligence services against critical information infrastructure of Ukraine under conditions of ongoing armed aggression. It is substantiated that modern cyberattacks against critical information

infrastructure are of a complex nature and should be understood not only as technical incidents, but also as a component of intelligence and subversive activities of foreign states in cyberspace. It is determined that effective counteraction to such threats requires a combination of technical cybersecurity measures and counterintelligence mechanisms aimed at prevention, detection, documentation, and neutralization of threat sources.

The activity of APT groups associated with foreign intelligence services is analyzed, and their role in the implementation of strategic cyber operations against Ukraine is revealed. A comparative analysis of critical infrastructure protection models in the United States, Israel, and the Republic of Estonia is carried out, which made it possible to establish the system-forming role of intelligence and counterintelligence agencies in ensuring cybersecurity. It is proved that effective national models are based on institutionalized intelligence sharing, public-private partnerships, and integration of civilian, military, and intelligence capabilities.

The current regulatory framework of Ukraine in the field of critical information infrastructure protection is analyzed, and its key shortcomings are identified, in particular the lack of proper institutional integration of counterintelligence activities into the cybersecurity system, insufficient effectiveness of mandatory cyber incident reporting mechanisms, and the absence of a legally established cyber reserve. The directions for improving legislation are proposed, including the introduction of mandatory intelligence-sharing mechanisms, strengthening counterintelligence powers in the field of critical infrastructure protection, development of a cyber reserve, and formation of legal frameworks for cyberattack attribution. It is concluded that there is a need to transition from a reactive to a proactive model of counterintelligence support for cybersecurity in Ukraine.

The obtained results have practical significance for improving state policy in the field of protection of critical information infrastructure and enhancing the effectiveness of the activities of the subjects of the national cybersecurity system of Ukraine.

Keywords: cybersecurity; critical information infrastructure objects; cyberattacks; counterintelligence activity; foreign intelligence services; cybercrime; cyberterrorism; national security; determinants; prevention.

Постановка проблеми. Захист об’єктів критичної інформаційної інфраструктури (далі – ОКІІ) є одним із ключових пріоритетів державної політики у сфері національної безпеки України в умовах тривалої збройної агресії російської федерації. Кібератаки на ОКІІ дедалі частіше набувають ознак систематичної, цілеспрямованої діяльності, що координується іноземними спеціальними службами з використанням спеціалізованих кіберзасобів, а відтак виходять за межі звичайних інцидентів інформаційної безпеки.

Особливістю зазначених загроз є їхня подвійна природа: технічна – як компрометація інформаційних систем, автоматизованих систем управління та мереж передачі даних, та розвідувальна – як інтегральна складова стратегічних операцій іноземних розвідувальних органів у кіберпросторі. Саме ця обставина зумовлює необхідність синтезу двох взаємодоповнювальних підходів до протидії: технічних та спеціальних контррозвідувальних заходів, спрямованих на попередження, виявлення, документування та нейтралізацію джерел загрози.

Разом із тим чинне законодавство – зокрема Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [1] – визначає загальні засади координації суб’єктів кібербезпеки, однак не встановлює конкретного механізму участі контррозвідувальних органів у захисті ОКІІ.

Це зумовлює нагальну потребу в концептуальному переосмисленні ролі контррозвідувальних органів – передусім Служби безпеки України у загальній системі захисту ОКІІ та розробленні відповідних законодавчих механізмів, що й становить предмет цього дослідження.

Мета дослідження. Метою статті є визначення місця і ролі контррозвідувальних органів у системі захисту об’єктів критичної інформаційної інфраструктури України від кібератак іноземних спецслужб, а також обґрунтування необхідності вдосконалення правового механізму їх участі у протидії розвідувально-підривній діяльності у кіберпросторі.

Стан опрацювання проблематики. Зважаючи на актуальність проблемних питань захисту об’єктів критичної інформаційної інфраструктури (ОКІІ) від кібератак іноземних спецслужб та їхнього впливу на національну безпеку, ця проблематика є предметом наукових дискусій як у національному, так і у зарубіжному науковому просторі.

Серед націоанальних науковців значний внесок у дослідження контррозвідувальних аспектів зробили К. Борисова, М. Грушко, М. Давиденко, Д. Дубов, А. Ільєнко, В. Кочин, О. Литвиненко, Я. Мануїлов, О. Мойко, Ю. Найдьон, М. Опанович, О. Пелюх, М. Погорецький, А. Тімошин, І Ткачов та інші. Їх дослідження охоплюють питання аналізу правового регулювання протидії розвідувально-

підривним операціям іноземних держав, а також проблематику інтеграції контррозвідувальних заходів у систему національної кібербезпеки.

На міжнародному рівні питання кібератак на критичну інфраструктуру та ролі спецслужб в їх протидії активно досліджують Д. Альперович (Dmitri Alperovitch), М.Дж. Ассанте (Michael J. Assante), М. Бредлі (Martha Bradley), Р. Бучан (Russell Buchan), Р.А. Кларк (Richard A. Clarke), Г. Корн (Gary Corn), Т. Конвей (Tim Conway), М. С. Коен (Michael S. Cohen), Г. Г. Діннісс (Heather Harrison Dinniss), Ч. Д. Фрейліх (Charles D. Freilich), Л. Гізель (Laurent Gisel), Дж. Горовіц (Jonathan Horowitz), Ч. Хуан (Zhixiong Huang), М. Хюппонен (Mikko Hypponen), Р. К. Кнейк (Robert K. Knake), Р. М. Лі (Robert M. Lee), К. Мачак (Kubo Mačák), Д. Массінгтон (David Mussington), Т. Роденхойзер (Tilman Rodenhäuser), Г. Сібоні (Gabriele Siboni), М. Н. Шмітт (Michael N. Schmitt) та інші.

Незважаючи на важливість дослідження захисту ОКІІ від атак іноземних спецслужб, наукові праці охоплюють лише окремі аспекти цієї проблематики, що вимагає подальших досліджень і підтверджує актуальність теми.

Виклад основного матеріалу. Захист об'єктів критичної інформаційної інфраструктури є пріоритетом національної безпеки України в умовах збройної агресії рф. З контррозвідувальної точки зору кібератаки на ОКІІ є інструментом реалізації розвідувально-підривних завдань іноземних спецслужб, що здійснюються через підконтрольні їм APT-групи (*Advanced Persistent Threat*). На відміну від «хакерів», APT-групи діють за оперативними завданнями розвідувальних відомств, мають значне ресурсне та технологічне забезпечення, а їхні операції плануються на місяці й роки вперед. Так, угруповання «Sandworm» та «Fancy Bear» діють в інтересах гру генерального штабу зс рф, «Gamaredon» – фсб росії. Їхня тактика передбачає поетапне проникнення в мережеву інфраструктуру: від первинної розвідки та фішингу до закріплення, горизонтального переміщення мережею та очікування команди на руйнівний напад у стратегічно важливий момент – наприклад, напередодні або під час активних бойових дій. М. Опанович доводить, що протидія операціям угруповань «Sandworm», «Fancy Bear» та «Gamaredon» вимагає не лише технічних засобів захисту мереж, а й комплексного вивчення тактик, технік і процедур (TTP) кожної групи, що фактично передбачає застосування розвідувальних та оперативно-аналітичних методів – тобто інструментарію, притаманного контррозвідувальній діяльності [2, с. 180]. М. Грушко констатує, що ефективне юридичне закріплення результатів атрибуції кібератак (технічної, публічної та правової) – наразі не забезпечене достатнім механізмом у національному законодавстві, що суттєво обмежує можливості правового реагування на розвідувально-підривну діяльність іноземних держав у кіберпросторі [3, с. 198].

Практика переконливо підтверджує системний і спланований характер кібероперацій рф на ОКІІ України. У грудні 2015 року угруповання «Sandworm» здійснило першу в світі підтверджену кібератаку на енергетичну інфраструктуру, застосувавши шкідливе програмне забезпечення «BlackEnergy» проти трьох обленерго – понад 230 000 споживачів залишилися без електропостачання у розпал зими [4]. У грудні 2016 року, та сама група атакувала «Укренерго», використавши значно складніший інструмент «Industroyer (Crashoverride)», здатний безпосередньо маніпулювати промисловими системами управління електромережею [5].

Обидва інциденти відбулися в координації з воєнними діями на сході нашої країни, що свідчить про їхній стратегічний, а не ситуативний характер. У січні-лютому 2022 року на системи державних органів та підприємств КІІ України було здійснено масові кібератаки із застосуванням wiper-програми «WhisperGate» та «HermeticWiper», що мали на меті знищення даних для дезорганізації управлінської вертикалі [6]. Показово, що попередня підготовка до атак тривала щонайменше кілька місяців – мала прихований доступ до частини систем задовго до активації шкідливого програмного забезпечення. Такі кейси демонструють, що кібератаки є складовою загального плану стратегії агресії та потребують контррозвідувального реагування.

Національна наукова думка формує концептуальне підґрунтя для розуміння природи зазначених загроз та шляхів протидії. О. Литвиненко зазначає, що кіберпростір є невід'ємним середовищем ведення сучасних операцій іноземних спецслужб, а ефективна відповідь вимагає переорієнтації оперативних ресурсів органів безпеки саме на протидію у цьому вимірі [7, с. 46]. Д. Дубов акцентує на необхідності системної роботи держави з виявлення загроз у кіберпросторі та вироблення механізмів захисту національних інтересів, що є неодмінною умовою своєчасного реагування з боку контррозвідувальних органів [8, с. 274]. І. Діордіца обґрунтовує необхідність запровадження у національному законодавстві України правової категорії «кібершпигунство» та вдосконалення на цій підставі механізмів кримінально-правової охорони державної таємниці, наголошуючи, що контррозвідувальні заходи СБ України є основним інструментом протидії відповідній діяльності спеціальних служб іноземних держав у кіберпросторі [9, с. 53]. М. Погорецький та В. Шеломенцев, досліджуючи правову природу кіберпростору як середовища вчинення злочинів, ще у 2009 році

обґрунтували необхідність формування спеціального понятійно-категоріального апарату для правової кваліфікації протиправних дій у цьому середовищі [10, с. 80] – що є передумовою належного юридичного забезпечення контррозвідувальної діяльності щодо захисту ОКІІ.

На важливості протидії кібератакам у цьому контексті зосереджено увагу й іноземних дослідників. Зокрема, Р. Кларк та Р. Кнейк (англ. – *Clarke R. A., Knake R. K.*) у фундаментальній праці «Кібервійна: наступна загроза національній безпеці та що з цим робити» (англ. – *Cyber War: The Next Threat to National Security and What to Do About It*) обґрунтували необхідність конвергенції розвідувальних та кібероперацій них спроможностей у межах єдиного командного контуру як умови ефективної протидії державним суб'єктам кібероперацій [11]. Ч. Фрейліх, М. Коен та Г. Сібоні (англ. – *Freilich C. D., Cohen M. S., Siboni G.*) у монографії «Ізраїль і кіберзагрози: як нація стартапів перетворилася на глобальну кібердержаву» (англ. – *Israel and the Cyber Threat: How the Startup Nation Became a Global Cyber Power*) на прикладі Ізраїлю демонструють, що модель безпосереднього залучення іноземними державами розвідувальних органів ефективно впливає на захист ОКІІ [12, с. 143].

Наведені наукові позиції свідчать про сформований у доктрині консенсус щодо необхідності інтеграції контррозвідувальних спроможностей у систему захисту ОКІІ. Водночас питання про конкретні організаційно-правові механізми такої інтеграції залишається відкритим. З метою його вирішення звернемося до міжнародного досвіду держав, які вже пройшли шлях від декларативного визнання кіберзагроз до побудови дієвих інституційних моделей взаємодії органів розвідки, контррозвідки та операторів ОКІІ.

Сформована модель захисту ОКІІ США ґрунтується на інституціоналізованому публічно-приватному партнерстві, центральним елементом якого є Агентство з кібербезпеки та захисту інфраструктури (далі – CISA). Принципова особливість цієї моделі полягає у поєднанні двох взаємодоповнювальних механізмів – обов'язкової звітності про інциденти та оперативного обміну розвідувальними даними про загрози в режимі реального часу.

Правовою основою обов'язкової звітності є *Cyber Incident Reporting for Critical Infrastructure Act of 2022* (CIRCIA) – Закон про звітування про кіберінциденти в критичній інфраструктурі 2022 року. Відповідно до його положень оператори критичної інфраструктури зобов'язані повідомляти CISA про кіберінциденти протягом 72 годин з моменту виявлення, а про здійснення виплат за програмами-вимагачами – протягом 24 годин [13]. У разі невиконання цих вимог CISA наділена повноваженнями вживати примусових заходів, зокрема видавати судові повістки та передавати матеріали до Міністерства юстиції для кримінального переслідування [14]. Отримані повідомлення дозволяють CISA оперативно розгортати ресурси для надання допомоги постраждалим, аналізувати звітність у різних секторах для виявлення потенційних загроз кібервпливів та поширювати цю інформацію серед захисників мереж з метою попередження інших потенційних жертв. За оцінками CISA, дія CIRCIA поширюється більш ніж на 300 000 суб'єктів господарської діяльності [15].

Паралельно з механізмом обов'язкової звітності функціонує оперативний механізм обміну розвідувальними даними – Спільна платформа кіберзахисту (далі – JCDC), створена CISA у серпні 2021 року на підставі *National Defense Authorization Act* 2021 року. JCDC забезпечує синхронізацію реагування на кіберінциденти через оперативний двосторонній та багатосторонній обмін інформацією про загрози, технічні й аналітичні обміни між партнерськими організаціями, а також розроблення операційних планів і посібників спільно з федеральними, промисловими та міжнародними партнерами [16]. До складу державних партнерів JCDC входять такі федеральні органи США, як Міністерство оборони США, Кіберкомандування США, Агентство національної безпеки, Міністерство юстиції США, Федеральне бюро розслідувань та Офіс директора національної розвідки. [17]. Таким чином, у межах Joint Cyber Defense Collaborative (JCDC) забезпечується інституціоналізована інтеграція розвідувальних спроможностей із системою захисту об'єктів критичної інформаційної інфраструктури, що фактично формує єдиний контур кіберзахисту; саме такий синергетичний підхід наразі залишається недостатньо розвиненим в українській моделі.

Дослідники наголошують на стратегічній ефективності такої моделі. Зокрема, К. Вайт (*англ. – Whyte C.*), А. Шерідан (*англ. – Sheridan A.*) та Т. Воттс (*англ. – Watts T.*) зазначають, що публічно-приватне партнерство є важливим інструментом підвищення спроможності держави до протидії сучасним кіберзагрозам, зокрема у контексті діяльності, пов'язаної з іноземними розвідувальними структурами, тоді як розвинена технологічна та кіберіндустрія формує додаткові переваги у цьому вимірі [18]. В. Адапа (*англ – Adapa V. R. K.*), аналізуючи стратегії кіберзахисту критичної інфраструктури, констатує, що інституціоналізований обмін розвідувальними даними про загрози між державними структурами та операторами ОКІІ є ключовим елементом адаптивної системи захисту, здатної реагувати на еволюцію тактик державних органів кібероперацій [19, с. 83].

Ізраїльська модель захисту об'єктів критичної інформаційної інфраструктури (ОКІІ) формувалася поступово з початку 2000-х років і ґрунтується на принципі глибокої інтеграції розвідувальних, військових і цивільних кіберспроможностей. Ще в лютому 2002 року уряд Держави Ізраїль ухвалив Резолюцію B/84, якою передбачено організацію захисту критичної інфраструктури та покладено відповідні повноваження на Службу внутрішньої безпеки Ізраїлю (Шабак, англ. – Shin Bet) [20]. Таким чином, від самого початку система захисту ОКІІ в Ізраїлі була інституційно інтегрована з контррозвідувальним органом, а не обмежувалася виключно функціонуванням технічних суб'єктів кіберзахисту.

Координатором цивільного кіберзахисту є Національний кібердиректорат (далі – INCD), створений у 2018 році шляхом злиття Національного кібербюро та Національного органу з кібербезпеки і підпорядкований безпосередньо Офісу прем'єр-міністра. INCD є національним органом безпеки та технологічним агентством, відповідальним за захист національного кіберпростору та розбудову кіберпотенціалу держави; він діє на національному рівні з метою постійного підвищення рівня захисту організацій і громадян, запобігання кібератакам та реагування на них, а також зміцнення спроможностей реагування на надзвичайні ситуації [21].

Ключовою особливістю ізраїльської моделі є системний механізм трансферу розвідувальних спроможностей і технологій із військового сектору до цивільного. В основі кіберструктури Держави Ізраїль перебувають три ключові елементи: підрозділ 8200, Директорат C4I (зокрема підрозділи кіберзахисту) та цивільний орган – Національний кібердиректорат Ізраїлю (*англ. – Israel National Cyber Directorate, INCD*); водночас служби зовнішньої та внутрішньої розвідки – Моссад (*англ. – Mossad*) і Шабак (*англ. – Shin Bet*) – також здійснюють активну кібердіяльність [22]. Важливим елементом цієї моделі є кадрово-технологічна дифузія: колишні співробітники підрозділу 8200 заснували такі провідні компанії, як Check Point, CyberArk, Claroty, CyCognito та Palo Alto Networks, які одночасно функціонують як суб'єкти глобального кіберринку та елементи національної системи кібербезпеки [23]. Таким чином, відбувається інституціоналізований процес перенесення розвідувальних технологій і методів у приватний сектор, що забезпечує безперервне підсилення системи захисту ОКІІ.

INCD координує анонімну платформу обміну інформацією, що дозволяє силам оборони взаємодіяти з приватним сектором. Важливо, що приватні підприємства та державні установи, що перебувають під наглядом, несуть фінансову відповідальність за всі операції, захист та відновлення своїх критичних інформаційних систем, водночас зобов'язані ділитися інформацією з регулятором; законом передбачені санкції проти керівників організацій, що нехтують обов'язковими вимогами.

Суттєвою відмінністю ізраїльської моделі від американської є те, що функція захисту ОКІІ від зовнішніх кіберзагроз перебуває в інституційній площині не лише технічного регулювання, а й діяльності спеціальних служб. Служба внутрішньої безпеки Ізраїлю – Шабак, поряд із INCD, здійснює повноваження у сфері кіберзахисту та підзвітна безпосередньо прем'єр-міністру. Зокрема, на Шабак покладено функції забезпечення кіберзахисту стратегічних телекомунікаційних операторів відповідно до законодавства про регулювання безпеки в публічному секторі [24]. Це означає, що контррозвідувальний орган Ізраїлю є не допоміжним суб'єктом, а безпосереднім учасником системи захисту ОКІІ, що принципово відрізняє ізраїльський підхід від нинішньої моделі в Україні.

Естонська модель захисту ОКІІ сформувалася як відповідь на масштабні DDoS-атаки 2007 року, які вперше актуалізували кіберзагрози як складову національної безпеки та зумовили переосмислення ролі держави у сфері кіберзахисту. Правовою основою цієї моделі є Закон Естонської Республіки про кібербезпеку (*Küberturvalisuse seadus*), який визначає Орган інформаційних систем (*англ. – Estonian Information System Authority, RIA*) як національний компетентний орган та єдину точку контакту у сфері кібербезпеки, зокрема для координації реагування на кіберінциденти, обміну інформацією про кіберзагрози, взаємодії з суб'єктами критичної інфраструктури, а також забезпечення міжнародної співпраці в межах ЄС і з партнерами у сфері кіберзахисту [25].

Ключовим елементом естонської моделі є Підрозділ кіберзахисту Ліги оборони Естонії (*англ. – Estonian Defence League's Cyber Unit, KKL)* – добровільне об'єднання висококваліфікованих ІТ-фахівців, інституційно інтегроване у систему національної оборони, яке забезпечує ефективну цивільно-військову взаємодію у сфері протидії кіберзагрозам, зокрема в умовах кризових ситуацій [26; 27].

Таким чином, естонська модель характеризується поєднанням централізованої координації через Орган інформаційних систем (RIA) та децентралізованого залучення приватного сектору і волонтерських спроможностей, що формує багаторівневу, адаптивну систему захисту ОКІІ. У її основі лежить концепція «whole-of-society approach», яка передбачає інтеграцію державних органів, бізнесу та громадянського суспільства до єдиної системи забезпечення кібербезпеки [28].

Як зазначають Е. Тікк (*англ. – Tikk E.*), К. Каска (*англ. – Kaska K.*) та Л. Віхул (*англ. – Vihul L.*), саме події 2007 року зумовили формування в Естонії цілісної правової, стратегічної та організаційної системи кібербезпеки, що базується на інтеграції державних інституцій, чіткій нормативній регламентації та розвитку міжнародного співробітництва у сфері кіберзахисту [29].

Проведений компаративістський аналіз дозволив виявити три перевірені практикою моделі залучення органів розвідки та контррозвідки у систему захисту ОКІІ. Відбір зазначених моделей зумовлений їхньою релевантністю для українського контексту: кожна з них сформувалася у відповідь на реальні загрози з боку державних суб'єктів кібероперацій, пройшла практичну апробацію в умовах кризових ситуацій та містить елементи, придатні для імплементації в національне законодавство України. При цьому порівняльний аналіз здійснювався за такими критеріями: правова основа залучення розвідувальних та контррозвідувальних органів до захисту ОКІІ; механізм обміну інформацією між державними структурами безпеки та операторами ОКІІ; наявність інституційного зв'язку між спецслужбами і приватним сектором; ступінь юридичної обов'язковості участі операторів ОКІІ у загальнодержавній системі кіберзахисту. Встановлено, що в усіх трьох моделях – американській, ізраїльській та естонській, контррозвідувальні органи виконують не допоміжну, а системоутворювальну функцію, забезпечуючи розвідувальне супроводження захисту ОКІІ на стратегічному та оперативному рівнях.

Правову основу захисту ОКІІ в Україні становить комплекс взаємопов'язаних законодавчих і підзаконних нормативно-правових актів. Базовим актом є Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [1], який визначає правові та організаційні засади забезпечення кібербезпеки, а також систему суб'єктів національної системи кібербезпеки та їх повноваження.

Захист критичної інфраструктури в цілому врегульовано Законом України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX [30], який закладає інституційні основи функціонування системи захисту критичних об'єктів. Стратегічні орієнтири державної політики у цій сфері визначені Стратегією кібербезпеки України, затвердженою Указом Президента України від 26.08.2021 № 447/2021 [31], у якій серед ключових загроз виокремлено організовані та підтримувані іноземними державами кібератаки, пов'язані зі здійсненням розвідувально-підривної діяльності.

Контррозвідувальні повноваження у сфері кібербезпеки покладено на Службу безпеки України відповідно до Закону України «Про контррозвідувальну діяльність» від 26.12.2002 № 374-IV [32]. Розподіл функцій між суб'єктами кіберзахисту ОКІІ деталізовано у статті 8 Закону № 2163-VIII [1], відповідно до якої Державна служба спеціального зв'язку та захисту інформації України здійснює координацію діяльності суб'єктів кібербезпеки та забезпечує функціонування урядової команди реагування на комп'ютерні надзвичайні події CERT-UA, тоді як СБУ реалізує контррозвідувальні заходи з протидії кібершпигунству, кібердиверсіям і кібертероризму, у тому числі шляхом проведення спеціальних перевірок готовності ОКІІ до кіберзагроз.

Водночас постановою Кабінету Міністрів України від 19.06.2019 № 518 [33] встановлено обов'язок суб'єктів господарювання, що належать до ОКІІ, здійснювати невідкладне інформування CERT-UA та відповідних підрозділів СБУ про кіберінциденти та кібератаки.

Разом із тим чинна модель має переважно адміністративно-технічний характер реагування, оскільки механізми інституційної інтеграції контррозвідувальної діяльності до системи захисту ОКІІ залишаються недостатньо деталізованими на законодавчому рівні; обов'язок повідомлення про кіберінциденти не супроводжується ефективними інструментами примусового виконання, а залучення підготовленого резерву фахівців приватного сектору до забезпечення кіберзахисту ОКІІ не отримало належного нормативного закріплення.

Висновки. Проведене дослідження підтверджує, що кібератаки на об'єкти критичної інформаційної інфраструктури України, що здійснюються APT-угрупованнями «Sandworm», «Fancy Bear» та «Gamaredon», є не самостійними технічними інцидентами, а складовою розвідувально-підривної діяльності спеціальних служб іноземних держав у кіберпросторі. Їхній стратегічний, заздалегідь спланований характер свідчить про те, що підготовка до руйнівних кібероперацій здійснюється задовго до їх активації, а самі атаки координуються з перебігом збройного протистояння. Це означає, що ефективна відповідь на зазначені загрози принципово не може обмежуватися суто технічними заходами кіберзахисту і потребує повноцінного контррозвідувального реагування – виявлення, документування та нейтралізації загрози ще на етапі її підготовки.

Порівняльний аналіз американської, ізраїльської та естонської моделей переконливо підтверджує, що у державах, які зіткнулися з реальними кіберзагрозами з боку іноземних держав, контррозвідувальні органи виконують не допоміжну, а системоутворювальну роль у захисті ОКІІ. В американській моделі це реалізовано через інституціоналізований механізм JCDC, що забезпечує інтеграцію розвідувальних спроможностей АНБ, ФБР та Кіберкомандування зі системою захисту операторів ОКІІ,

а юридично обов'язкова звітність про інциденти підкріплена реальними санкціями. В ізраїльській – через пряме законодавче закріплення повноважень Шабаку щодо захисту стратегічних телекомунікаційних операторів, що перетворює контррозвідувальний орган із суб'єкта реагування на безпосереднього учасника системи кіберзахисту. В естонській – через інституційне включення добровільного кіберрезерву, сформованого з фахівців приватного сектору та інтегрованого до системи національної оборони, що забезпечує стійкість держави в умовах кризових ситуацій. Спільною рисою всіх трьох моделей є проактивна, а не реактивна роль спеціальних служб у захисті ОКІІ.

Чинна українська модель захисту ОКІІ, попри наявність відповідної нормативно-правової бази, має переважно адміністративно-технічний характер. СБУ визначена суб'єктом кібербезпеки з контррозвідувальними функціями, однак механізм її інституційної інтеграції до системи захисту конкретних категорій ОКІІ залишається недостатньо деталізованим. Обов'язок операторів повідомляти про кіберінциденти не підкріплений ефективними інструментами примусового виконання. Інститут кіберрезерву з числа фахівців приватного сектору, попередньо перевірених і підготовлених спеціальними службами, відсутній. Механізм юридичного закріплення результатів атрибуції кібератак, необхідний для притягнення до відповідальності держав – суб'єктів кібероперацій, залишається нерозвиненим. Усе це не дозволяє системі в її нинішньому вигляді здійснити перехід від реагування на вже здійснені атаки до їх попередження.

Усунення зазначених прогалин потребує реалізації комплексу взаємопов'язаних заходів. На законодавчому рівні необхідно закріпити механізм обов'язкового та невідкладного обміну розвідувальними даними про кіберзагрози між СБУ, CERT-UA та операторами ОКІІ за моделлю американської JCDC, встановивши юридичну відповідальність за ухилення від повідомлення про кіберінциденти. У профільному законодавстві слід конкретизувати превентивні контррозвідувальні повноваження СБУ щодо захисту окремих категорій ОКІІ, зосередивши їх на виявленні та нейтралізації загрози на етапі її підготовки – за прикладом ізраїльської моделі. Запровадження інституту кіберрезерву з числа фахівців приватного ІТ-сектору, попередньо перевірених і підготовлених органами СБУ, забезпечить додаткові спроможності держави у кризових ситуаціях за естонським зразком. Окремої уваги потребує формування дієвого правового механізму атрибуції кібератак на ОКІІ з юридичним закріпленням її результатів як передумови застосування заходів міжнародно-правової відповідальності до держав – суб'єктів кібероперацій.

Реалізація зазначених заходів дозволить здійснити перехід від моделі реактивного реагування до проактивного контррозвідувального захисту ОКІІ – виявлення і нейтралізації загроз на етапі їх підготовки, що відповідає кращим стандартам міжнародного досвіду та завданням забезпечення національної безпеки України в умовах триваючої збройної агресії.

Водночас проведене дослідження окреслює коло питань, що потребують подальшого наукового опрацювання. Зокрема, поза межами цієї роботи залишилися проблеми правового регулювання активних контррозвідувальних заходів у кіберпросторі, механізмів міжнародного співробітництва спеціальних служб у сфері захисту ОКІІ, а також питання стандартизації вимог кіберзахисту для різних категорій операторів критичної інфраструктури. Зазначені напрями становлять самостійний науковий інтерес і потребують окремого дослідження з метою формування цілісної та ефективної системи контррозвідувального захисту об'єктів критичної інформаційної інфраструктури України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
2. Опанович М. Аналіз кібератак та діяльності APT груп в Україні. *Кібербезпека: освіта, наука, техніка*. 2024. Т. 4, № 24. С. 172–184. DOI: https://doi.org/10.28925/2663-4023.2024.24.172184.
3. Грушко М.В. Атрибуція кібератак як передумова забезпечення відповідальної поведінки в кіберпросторі. *Правова держава*. 2021. № 43. DOI: https://doi.org/10.18524/2411-2054.2021.43.241002.
4. Cybersecurity and Infrastructure Security Agency. (2016, February 25; last revised July 20, 2021). Cyber-Attack Against Ukrainian Critical Infrastructure (Alert IR-ALERT-H-16-056-01). U.S. Department of Homeland Security. URL: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.
5. Lee, R.M., Assante, M.J., & Conway, T. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. Electricity Information Sharing and Analysis Center (E-ISAC) & SANS Institute. URL: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf.

6. Cybersecurity and Infrastructure Security Agency & Federal Bureau of Investigation. (2022, February 26; updated April 28, 2022). Update: Destructive Malware Targeting Organizations in Ukraine (Alert AA22-057A). U.S. Department of Homeland Security & U.S. Department of Justice. URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a.
7. Литвиненко О. Тотальна війна по-путінські: «гібридна» війна РФ проти України. *«Гібридна» війна Росії – виклик і загроза для Європи* : зб. матеріалів. Центр Разумкова. Київ, 2016. С. 45–49. URL: https://razumkov.org.ua/images/Material_Conference/2016_12_14/GIBRID-WAR-FINAL-1-1.pdf.
8. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ: НІСД, 2014. 328 с. URL: https://www.niss.gov.ua/sites/default/files/2015-02/Dubov_mon-89e8e.pdf.
9. Діордіца І.В. Поняття та зміст кібершпигунства. *Наукові праці Національного університету «Одеська юридична академія»*. 2020. Вип. 26. С. 49--55. URL: http://naukovipraci.nuoua.od.ua/arhiv/tom26/9.pdf.
10. Погорецький М.А., Шеломенцев В.П. Поняття кіберпростору як середовища вчинення злочинів. *Інформаційна безпека людини, суспільства, держави*. 2009. № 2 (2). С. 77–81. URL: https://ir.library.knu.ua/server/api/core/bitstreams/ec85c21d-aef8-45ca-bad9-5932fd25a727/content.
11. Clarke R.A., Knake R.K. Cyber War: The Next Threat to National Security and What to Do About It. New York : HarperCollins/Ecco, 2010. 304 p. URL: https://www.amazon.com/Cyber-War-Threat-National-Security/dp/0061962244.
12. Freilich C.D., Cohen M.S., Siboni G. Israel and the Cyber Threat: How the Startup Nation Became a Global Cyber Power. New York: Oxford University Press, 2023. 424 p. URL: https://academic.oup.com/book/46512.
13. Cybersecurity and Infrastructure Security Agency. Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). URL: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.
14. Kohne N.G., Hold J. New CISA Cybersecurity Incident Reporting Requirements Proposed for Critical Infrastructure Companies. 2024. URL: https://www.akingump.com/en/insights/blogs/ag-data-dive/new-cisa-cybersecurity-incident-reporting-requirements-proposed-for-critical-infrastructure-companies.
15. Ringrose K., Reynolds S., Ravi S. The clock starts soon: Preparing for CIRCIA. *International Association of Privacy Professionals (IAPP)*. 2024. URL: https://iapp.org/news/a/the-clock-starts-soon-preparing-for-circia.
16. Cybersecurity and Infrastructure Security Agency. Joint Cyber Defense Collaborative (JCDC). URL: https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative.
17. Cybersecurity and Infrastructure Security Agency. CISA Launches New Joint Cyber Defense Collaborative. 2021. URL: https://www.cisa.gov/news-events/news/cisa-launches-new-joint-cyber-defense-collaborative.
18. Whyte C., Sheridan A., Watts T. Private-public initiatives for cybersecurity: the case of Ukraine. *Journal of Cyber Policy*. 2025. DOI: https://doi.org/10.1080/23738871.2025.2451256.
19. Adapa V. R. K. Cybersecurity Strategies for Critical Infrastructure: Defending National Security and Ensuring Resilience. *International Journal of Information Technology and Management Information Systems (IJITMIS)*. 2024. Vol. 15, № 2. P. 75-84. DOI: https://doi.org/10.5281/zenodo.14376549.
20. National Cyber Security Authority (Israel). Wikipedia. URL: https://en.wikipedia.org/wiki/National_Cyber_Security_Authority_(Israel).
21. Israel National Cyber Directorate (INCD). Cybil Portal. URL: https://cybilportal.org/actors/cyber-israel-national-cyber-directorate.
22. Olech A., Kwaśniewska D. Cyber Forces: Israel. Defence24. URL: https://defence24.com/geopolitics/cyber-forces-israel.
23. Tabansky L. Israel Defense Forces and National Cyber Defense. Connections: The Quarterly Journal. 2020. Vol. 19. № 1. P. 45–62. DOI: https://doi.org/10.11610/Connections.19.1.05 URL: https://connections-qj.org/system/files/19.1.05_cyber_defence_israel.pdf?download=1.
24. The Cyber Defense Organizations Protecting Israel's Critical Infrastructure. National Institute for Defense Studies 2022. URL: https://www.nids.mod.go.jp/english/publication/briefing/pdf/2022/briefing_e202201.pdf.
25. NATO Strategic Communications Centre of Excellence. 2007 Cyber Attacks on Estonia. URL: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf.

26. Estonian Information System Authority (RIA). Cyber Defence of Critical Infrastructure. URL: https://www.ria.ee/en/cyber-security/cyber-defence-critical-infrastructure.
27. Estonian Defence League Act. Riigi Teataja. URL: https://www.riigiteataja.ee/en/eli/521032014005/consolide.
28. Digital Front Lines. Lessons from Estonia's Whole-of-Society Approach to Cyber Defense. 2023. URL: https://digitalfrontlines.io/2023/08/31/lessons-from-estonias-whole-of-society-approach-to-cyber-defense.
29. Tikk E., Kaska K., Vihul L. Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. *Journal of Cyber Warfare and Terrorism*. 2011. Vol. 1, № 1. URL: https://ccdcoe.org/library/publications/estonia-after-the-2007-cyber-attacks-legal-strategic-and-organisational-changes-in-cyber-security.
30. Про критичну інфраструктуру. Закон України від 16.11.2021 № 1882-IX. *Відомості Верховної Ради України*. 2022. № 2. Ст. 14 URL: https://zakon.rada.gov.ua/laws/show/1882-20-Text.
31. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.
32. Про контррозвідувальну діяльність. Закон України від 26.12.2002 № 374-IV. *Відомості Верховної Ради України*. 2003. № 12. Ст. 89 URL: https://zakon.rada.gov.ua/laws/show/374-15#Text.
33. Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури. Постанова Кабінету Міністрів України від 19.06.2019 № 518. *Офіційний вісник України.* 2019. № 52. Ст. 1780 URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.

Дата першого надходження рукопису до видання: 1.03.2026
Дата прийняття до друку рукопису після рецензування: 20.03.2026
Дата публікації: 5.03.2026

© Погорецький М.М., Клименко С.В., 2026
Стаття поширюється на умовах ліцензії CC BY 4.0