УДК 342.951

МАНУІЛОВ Я.С., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-8149-2745.

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ КІБЕРВІЙНИ

Анотація. *Визначено поняття та ознаки об'єктів критичної інфраструктури. Висвітлено роль та місце об'єктів критичної інфраструктури в структурі національної безпеки України. Деталізовані фактори, які впливають на захищеність об'єктів критичної інфраструктури.Окреслено засади державної політики у сфері забезпечення кібербезпеки об'єктів критичної інфраструктури. Визначено загрози, які впливають на захищеність об'єктів критичної інфраструктури в умовах кібервійни. Обгрунтовано доцільність проведення періодичних оглядів стану кібербезпеки об'єктів критичної інфраструктури стратегічних галузей економіки. Визначено шляхи та напрями забезпечення безпеки об'єктів критичної інфраструктури на державному рівні. Деталізовано перелік галузевих об'єктів критичної інфраструктури та визначено секторальні вимоги кібербезпеки щодо таких об'єктів. Узагальнено систему заходів, які спрямовані на посилення захисту об'єктів критичної інфраструктури від кібератак російських окупантів. Розкрито роль та завдання вітчизняної спецслужби у сфері контррозвідувального захисту об'єктів критичної інфраструктури. Проведено огляд вітчизняного законодавства з питань захисту об'єктів критичної інфраструктури. Визначено шляхи удосконалення вітчизняного законодавства з метою посилення стану забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах правового режиму воєнного стану.*

Ключові слова: *кібератака, критична інфраструктура, об'єкти критичної інфраструктури, державна політика у сфері кібербезпеки, секторальні вимоги кібербезпеки, кіберзахист, технологічна інфраструктура кіберзахисту, кібервійна, огляд стану кібербезпеки, паливо-енергетичний сектор, спецслужба,національна безпека,уповноважений державний орган з питань захисту критичної інфраструктуриє.*

Summary*. The concepts and characteristics of critical infrastructure are defined. The role and place of critical infrastructure in the structure of national security of Ukraine is highlighted. The factors that affect the security of critical infrastructure are detailed. The principles of state policy in the field of cyber security of critical infrastructure are outlined. The threats that affect the security of critical infrastructure in the conditions of cyber warfare have been identified. The expediency of conducting periodic reviews of the state of cyber security of critical infrastructure of strategic sectors of the economy is substantiated. The ways and directions of ensuring the safety of critical infrastructure at the state level have been determined. The list of sectoral objects of critical infrastructure is detailed and the sectoral cyber security requirements for such objects are defined. The system of measures aimed at strengthening the protection of critical infrastructure against cyberattacks by the Russian occupiers is summarized. The role and tasks of the domestic special service in the field of counter-intelligence protection of critical infrastructure are revealed. A fragmentary review of domestic legislation devoted to strengthening the protection of critical infrastructure was conducted. The directions of improvements of the domestic legislation in order to strengthen the state of ensuring cyber security of critical infrastructure under the conditions of the martial law have been determined.*

Keywords*:cyber attack, critical infrastructure, critical infrastructure objects, state policy in the field of cyber security, sectoral requirements of cyber security, cyber defense, technological infrastructure of cyber defense, cyber warfare, review of the state of cyber security, fuel and energy sector, special service, national security, authorized state body for the protection of critical infrastructure.*

Постановка проблеми. В сучасних умовах стійкі тенденції збільшення кількості загроз національній безпеці у кіберпросторі, які спостерігались протягом останніх років, лише посилились у зв'язку із здійсненням військової агресії РФ проти України. Так, повномасштабне вторгнення російських військ на територію України, що триває із 24 лютого 2022 року, супроводжується численними актами агресії у кіберпросторі. Триває масштабна кібервійна Російської Федерації проти України, важливим елементом якої є також акції кібервпливу, залишаючись найбільшою загрозою національній безпеці держави. В цьому контексті важливою складовою функціонування національної системи кібербезпеки є забезпечення безпеки саме об'єктів критичної інфраструктури,посилення спроможностей складових сектору безпеки і оборони, державних органів адекватно та випереджено реагувати на кіберзагрози.

В умовах повномасштабної війни РФ проти України захист об'єктів критичної інфраструктури залишається одним із важливих пріоритетів нашої держави. В сучасних умовах відбувається й кібервійна, у зв'язку з чим ризики для інфраструктури суттєво зростають. Адже саме від стану захищеності її об'єктів багато у чому залежить і національна безпека. Тому численні та цілеспрямовані кібератаки ворога спрямовані,у першу чергу, на підрив основ національної безпеки України, насамперед, шляхом заподіяння шкоди державним інформаційним ресурсам та вітчизняним об'єктам критичної інфраструктури.

Відповідно до положень Стратегії кібербезпеки України, затвердженої Указом Президента України від 26.08.21 р. № 447/2021 [15], забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Серед основних передумов та чинників, що формують загрози кібербезпеці України, на законодавчому рівні виділяються: недостатня захищеність від кібератак державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури; невідповідність вимогам законодавства стану захисту інформаційно-комунікаційних систем державних органів та суб'єктів господарювання, в яких обробляється значна частина інформації з обмеженим доступом тощо. Також негативний вплив на безпеку об'єктів критичної інфраструктури уможливлюється через ризик виникнення аварійних ситуацій або аварій внаслідок можливих кібератак. Виникнення аварійних ситуацій через кібератаки може призвести до значних матеріальних збитків,значної шкоди здоров'ю персоналу та населенню, суттєвих витрат на ліквідацію наслідків аварії, що є актуальним особливо в умовах російського вторгнення.

Враховуючи вищеназвані чинники, усунення яких є конче необхідним для зменшення масштабування загроз кібербезпеці України, а також нагальну потребу в посиленні спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури, необхідним є розробка й удосконалення організаційно-технічних, оперативних та правових механізмів з метою стримування збройної агресії РФ у кіберпросторі та одночасного надання гідної відсічі державі-агресору в умовах ведення активної фази кібервійни.

За таких умов актуальним та своєчасним є проведення дослідження з метою висвітлення проблемних питань забезпечення кібербезпеки об'єктів критичної

інфраструктури, особливо в умовах ведення кібервійни, визначення результатів й здобутків діяльності вітчизняної спецслужби за напрямом контррозвідувального захисту об'єктів критичної інфраструктури, визначення шляхів удосконалення правового регулювання вказаної сфери.

Результати аналізу наукових публікацій. Сучасний стан кримінально-правової охорони об'єктів критичної інфраструктури в Україні ретельно розглядали у своїх наукових працях С. Кучерина та Д. Олейніков [7], О. Суходоля [9]. Організаційно-правові засади забезпечення захисту критичної інфраструктури досліджували Ю. Березdецький та М. Пальчик [1], Н. Кідалова [4], М. Ковалів [5], Д. Павлов, М. Микитюк [10], С. Теленик [11], С. Цяпа [12]. Розробка методологічних основ оцінки ризиків щодо об'єктів критичної інфраструктури перебували у фокусі уваги О. Іваненка [3] та Ю. Когута [6]. Проте проблемні питання забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах ведення кібервійни та триваючого правового режиму військового стану, особливості контррозвідувального захисту таких об'єктів предметно залишилися поза межами уваги вказаних авторів, що підкреслює актуальність обраної тематики цієї статті.

Метою статті є визначення та масштабування загрозливих тенденцій поширення російського деструктивного контенту в умовах правового режиму військового стану, огляд діяльності вітчизняної спецслужби у зазначеній сфері, визначення шляхів удосконалення чинного законодавства з питань протидії деструктивному контенту.

Виклад основного матеріалу. Державна політика у сфері кібербезпеки визначається сукупністю нормативно-правових актів, що формують засади реалізації такої політики, її напрями, принципи та основні завдання. До ключових нормативних документів, що формують базовий рівень такої політики, належать Стратегія кібербезпеки України [15], закони України "Про основні засади кібербезпеки України" [16], "Про національну безпеку України" [17], "Про критичну інфраструктуру" [18], а також постанови Кабінету Міністрів України "Про затвердження Положення про організаційно-технічну модель кіберзахисту" [19], "Деякі питання об'єктів критичної інформаційної інфраструктури" [20], "Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом" [21], "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" [22] тощо. Більшість норм та положень цих правових актів повністю або частково присвячені проблематиці побудови сучасного та надійного забезпечення кіберзахисту об'єктів критичної інфраструктури.

Зокрема, у 2018 році набрав чинності Закон України "Про основні засади забезпечення кібербезпеки України" [16], дія якого, зокрема, поширюється на об'єкти критичної інфраструктури. Відповідно до пункту 2 частини третьої статті 8 цього закону для функціонування національної системи кібербезпеки необхідне створення відповідної нормативно-правової бази у сфері кібербезпеки з урахуванням гармонізації нормативних актів відповідно до міжнародних стандартів.

Передовий міжнародний досвід переконливо засвідчує, що за останні роки у світі в 57 разів збільшилася кількість кібератак, у зв'язку з чим провідні країни змушені посилювати захист стратегічно важливих підприємств та об'єктів критичної інфраструктури. Наразі найрозвиненіші держави світу витрачають на кібербезпеку у 5 разів більше, ніж на інші напрямки ІТ-галузі. За оцінками фахівців, вже у 2025 році ці витрати можуть сягнути 10,5 трильйонів доларів у світових масштабах.

Одним із основних чинників, які утворюють значну небезпеку об’єктам критичної інфраструктури, є кіберзагрози та кібератаки. Російська Федерація залишається одним із основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, яка базується на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у кібервійні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно об’єктів критичної інфраструктури.

24 лютого 2022 року держава-агресор віроломно та нахабно розпочала військову агресію проти держави Україна. У квітні 2022 року відбулася масштабна цільова кібератака РФ на об’єкти критичної інфраструктури. На жаль, російські кібератаки тривають на перманентній основі. Злочинний задум російських хакерів передбачав виведення з ладу високовольтних електричних підстанцій, комп’ютерів користувачів, серверів, автоматизованих робочих місць, серверного обладнання, активного мережевого обладнання тощо. Така кризова ситуація зумовлює необхідність покращення стану кібербезпеки, підвищення захищеності інформаційних ресурсів та інформаційно-комунікаційних систем об’єктів критичної інфраструктури в цілому до рівня, який забезпечує функціонування єдиного секторального (галузевого) безпечного інтегрованого інформаційного та комунікаційного середовища.

Слід вказати, що 29 грудня 2021 року Уряд України ухвалив “Положення про організаційно-технічну модель кіберзахисту”, яке затверджено постановою Кабінету Міністрів України № 1426 [19]. Нормативно встановлено, що організаційно-технічна модель передбачає три рівні інтегрованих інфраструктур кіберзахисту: організаційно-керівна (основні суб’єкти національної системи кібербезпеки);технологічна (взаємодія технологічних підрозділів, тобто обмін інформацією, моніторинг, забезпечення сталої безпеки кіберпростору тощо); базова (захищена інформаційна інфраструктура та суспільство (громада)). У свою чергу, організаційно-технічна модель кіберзахисту спрямована на забезпечення: підвищення функціонування системи кіберзахисту України та посилення координації дій між основними суб’єктами кібербезпеки; зменшення вразливості інформаційних, комунікаційних систем і забезпечення їх кіберстійкості; створення умов розвитку державно-приватного партнерства у сфері кібербезпеки; створення ефективної системи національного реагування на кіберінциденти, зокрема розвиток галузевих команд реагування, синхронізація та узгодження їхніх дій; підвищення національного потенціалу в галузі кібербезпеки в кіберпросторі; постійного контролю за станом кіберзахисту об’єктів критичної інфраструктури; конфіденційності, цілісності та доступності інформації, а також безпеки комунікаційних і технологічних систем.

Здійснення заходів з кіберзахисту передбачає: ідентифікацію – виявлення реальних і потенційних кіберзагроз для запобігання та їх нейтралізації; захист розроблення та впровадження методів, засобів, процедур кіберзахисту, спрямованих на забезпечення сталості і надійності функціонування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних та технологічних систем; виявлення – проведення моніторингу визначення, збору та обробки нетипових подій у кіберпросторі;реагування – вжиття заходів, спрямованих на запобігання кіберінцидентам, кібератакам, мінімізацію їх можливих наслідків (запобігання виникненню загроз життю або здоров’ю людей та заподіяння шкоди майну), удосконалення систем кіберзахисту, з урахуванням необхідності забезпечення пропорційності та співрозмірності можливостей таких систем реальним та потенційним ризикам; відновлення – поновлення штатного режиму

функціонування інформаційно-телекомунікаційних, технологічних систем після кібератаки, відновлення інформації та відомостей у разі їх пошкодження або видалення, створення передумов для проведення розслідування за наслідками кібератаки. Під час забезпечення функціонування базисної інфраструктури кіберзахисту має забезпечуватися захист у кіберпросторі національних електронних інформаційних ресурсів, комунікаційних і технологічних систем; захист об'єктів критичної інфраструктури; здійснення заходів з формування культури кібербезпеки на об'єктах критичної інфраструктури і підприємствах незалежно від форми власності; інформування громадян про наслідки кіберінцидентів.

Пунктом 8 Положення про організаційно-технічну модель кіберзахисту, затвердженого Постановою Кабінету Міністрів України від 29.12.21 р. № 1426 [19], визначено, що під час функціонування організаційно-керуючої інфраструктури кіберзахисту відповідальні суб'єкти забезпечення кібербезпеки організовують і проводять огляд стану кіберзахисту критичної інфраструктури. Метою проведення такого огляду є отримання об'єктивної та неупередженої інформації щодо оцінки рівня кібербезпеки та визначення напрямів удосконалення й розвитку системи кібербезпеки об'єктів критичної інфраструктури.

Таким чином, сьогодні держава активно опікується питаннями щодо впровадження та підвищення ефективності функціонування національної системи кібербезпеки об'єктів критичної інфраструктури з метою забезпечення сталого і безпечного функціонування національної критичної інфраструктури в кіберпросторі, створення передумов для об'єднання зусиль суб'єктів забезпечення кібербезпеки при вирішенні завдання підвищення рівня кіберстійкості критичної інфраструктури держави, яка охоплює як об'єкти критичної інфраструктури, так і комунікаційно-інформаційні та інші системи, сталість та надійність функціонування яких критично важлива для функціонування державних органів, підприємств, установ і організацій всіх форм власності, об'єднань громадян.

Виходячи із кращих практик зарубіжного досвіду, окрім основних суб'єктів національної системи кібербезпеки, до яких відносяться Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, сталою практикою у світі є запровадження уповноваженої відповідальної особи за захист критичної інфраструктури в органах на галузевому, регіональному рівні та на об'єктах критичної інфраструктури (Chief Information Security Officer, CISO) та наділення її повноваженнями, достатніми для прийняття управлінських рішень.

Силами кіберзахисту основних суб'єктів національної системи кібербезпеки є підрозділи, що безпосередньо здійснюють функції кіберзахисту в організаціях. Зокрема, Державний центр кіберзахисту (Держспецзв'язку), Ситуаційний центр (Служба безпеки України), Центр кіберзахисту (Національний банк України), Департамент кіберполіції Національної поліції України, відповідні підрозділи Міністерства оборони та Генерального штабу України. У національному координаційному центрі кібербезпеки РНБО України функцію сил кіберзахисту виконує технологічна платформа НКЦК РНБО. Прикладами представників галузевого рівня є Операційний центр безпеки (SOC) "Укренерго", кіберцентр "Нафтогазу", Державне підприємство "Галузевий центр цифровізації та кібербезпеки" Міністерства інфраструктури України тощо.

Забезпечення кібербезпеки об'єктів критичної інфраструктури передбачає масштабування технологічної інфраструктури кіберзахисту, який здійснюється за

рахунок поступового збільшення (відповідно до визначених вимог до таких суб'єктів) кількості елементів децентралізованої зони, їх підключення до суб'єктів централізованої зони та нарощування спроможностей інформаційно-технологічної взаємодії між ними. Обмін інформацією щодо кіберінцидентів відбувається на підставі міжвідомчих наказів, прийнятих протоколів обміну інформацією, з використанням TLP-протоколу та таксономії кіберінцидентів, у тому числі із використанням послуг платформи "Malware Information Sharing Platform", яка в режимі реального часу забезпечує обмін даними про кіберризики, атаки та інциденти на об'єктах критичної інфраструктури, в установах, на підприємствах і державних електронних інформаційних ресурсах. Ця платформа розгорнута між основними суб'єктами забезпечення кібербезпеки та до неї підключено більше ніж 500 підприємств, установ та організацій, більшу частину з яких можливо віднести до критичної інфраструктури України. Можливість підключення до цієї платформи станом на січень 2023 року надають Держспецзв'язку, Національний координаційний центр кібербезпеки, Ситуаційний центр кібербезпеки СБ України, MISP-NBU.

Головним завданням технологічної інфраструктури кіберзахисту є оперативний та ефективний захист кіберпростору в частині протидії кібератакам, кіберзлочинам, кібертероризму, кібершпигунству, в тому числі шляхом: збору, аналізу, оцінювання, узагальнення та поширення інформації про кіберінциденти; надання методичної допомоги іншим суб'єктам кіберзахисту; взаємного інформування суб'єктів кіберзахисту про нові реальні та потенційні загрози; створення умов для відповідального та довіреного обміну інформацією між суб'єктами кіберзахисту всіх секторів кіберзахисту.

Тобто актуальним та своєчасним у рамках посилення захисту об'єктів критичної інфраструктури є проведення огляду стану кібербезпеки відповідних секторів економіки України, наприклад паливно-енергетичного сектору. Це дозволить, у свою чергу, покращити стан кібербезпеки, підвищити захищеність інформаційних ресурсів та інформаційно-комунікаційних систем об'єктів критичної інфраструктури та паливно-енергетичного сектору в цілому до рівня, який забезпечує функціонування єдиного секторального (галузевого) безпечного інтегрованого інформаційного та комунікаційного середовища.

Під час проведення огляду очікувано потребуються додаткові витрати, пов'язані із реалізацією на об'єктах критичної інфраструктури комплексу заходів кіберзахисту, доцільних для приведення стану кібербезпеки у відповідність до нормативних вимог. Це надасть змогу значно підвищити безпеку та в майбутньому уникнути катастрофічних витрат, пов'язаних з ліквідацією наслідків аварій, що можуть виникнути внаслідок кібератак, спрямованих на об'єкти критичної інфраструктури. За результатами огляду можливо досягти із урахуванням сучасних міжнародних норм та вимог кібербезпеки конкретного цільового стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури, що значно зменшить ймовірність виникнення аварійних ситуацій та аварій (спричинених кібератаками) з вкрай негативними наслідками для держави, населення та навколишнього природного середовища.

Об'єктами огляду є оператори критичної інфраструктури, об'єкти критичної інфраструктури. Суб'єктами огляду є команди реагування на комп'ютерні надзвичайні події (інциденти комп'ютерної безпеки), підрозділи кіберзахисту та кібербезпеки оператора критичної інфраструктури, об'єкта критичної інфраструктури. Огляд проводиться з метою оцінювання стану кібербезпеки операторів критичної інфраструктури, об'єктів критичної інфраструктури та готовності суб'єктів огляду, до ефективного і оперативного реагування на кіберзагрози, попередження, виявлення та

захисту від кібератак і кіберінцидентів, ліквідації їх наслідків, відновлення функціонування операторів критичної інфраструктури, об’єктів критичної інфраструктури.

За результатами огляду визначаються напрями вдосконалення і розвитку системи кібербезпеки паливно-енергетичного сектору критичної інфраструктури в частині кіберзахисту з урахуванням реальних і потенційних загроз у кіберпросторі. Завданнями огляду є: проведення аналізу стану кіберзахисту операторів критичної інфраструктури, об’єктів критичної інфраструктури; розробка конкретизованих вимог з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування паливно-енергетичного сектору критичної інфраструктури; формування пропозицій щодо вдосконалення законодавства у сфері кібербезпеки, кіберзахисту та визначення напрямів розвитку системи кібербезпеки паливно-енергетичного сектору критичної інфраструктури в частині кіберзахисту; формування пропозицій щодо вдосконалення суб’єктами огляду заходів з кіберзахисту; планування заходів щодо забезпечення кіберстійкості операторів критичної інфраструктури, об’єктів критичної інфраструктури.

За наслідками проведення відповідного огляду готуються проекти внутрішніх наказів, у положеннях яких відображено систему (таксономію) заходів кіберзахисту для досягнення конкретного цільового стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури; визначаються рівні впровадження заходів кіберзахисту, що характеризують ступінь практичного впровадження оператором критичної інфраструктури заходів із кіберзахисту, здатність оператора критичної інфраструктури досягти запланованих результатів кіберзахисту та розкрити інструментарій оцінювання ступеня впровадження процесів управління кібербезпекою; визначаються профілі кіберзахисту, що використовуються для опису поточного стану реалізованих заходів кіберзахисту об’єктами критичної інфраструктури або бажаного цільового стану реалізації конкретних заходів кіберзахисту; деталізується загальна система правил обміну інформацією щодо кіберінцидентів.

Відповідно до ст. 5 Закону України “Про основні засади забезпечення кібербезпеки України” [16] Міністерство енергетики України є суб’єктом, що безпосередньо здійснює у межах своєї компетенції заходи із забезпечення кібербезпеки. Міненерго, за результатами узагальнення звітів про виконання плану заходів щодо усунення недоліків, виявлених під час огляду за рік складає відповідний звіт стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури та в десятиденний термін з дня його укладання надає Адміністрації Держспецзв’язку.

У 2019 році набрав чинності документ “Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури”, затверджений Постановою Кабінету Міністрів України від 19.06.19 р. № 518 [22]. Цей акт має загальний характер та стосується всіх об’єктів критичної інфраструктури усіх секторів критичної інфраструктури. Згідно з пунктом 14 цього акта міністерства та інші центральні органи виконавчої влади можуть розробляти конкретизовані вимоги з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування об’єктів критичної інфраструктури, які відносяться до сфери їх управління. Зважаючи на це, з урахуванням положень пункту 14 Загальних вимог було прийнято рішення щодо розроблення секторальних (галузевих) вимог з кібербезпеки паливно-енергетичного сектору критичної інфраструктури, які мають враховувати міжнародний досвід із кіберзахисту об’єктів критичної інформаційної інфраструктури в паливно-енергетичному секторі критичної інфраструктури, що зумовлено необхідністю визначення та врегулювання заходів кіберзахисту об’єктів критичної інфраструктури для досягнення конкретного цільового стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури.

Цілком логічно, що окреслена проблема не може бути вирішена за допомогою ринкових механізмів, оскільки визначення критеріїв і вимог безпеки, додержання яких обов'язкове у сфері кібербезпеки, можливе лише за допомогою державного регулювання. Про це вказував С. Теленику у своєму монографічному дослідженні [11].

Останнім часом російські війська посилили обстріли об'єктів енергетичної інфраструктури України. Для атак вони використовують крилаті ракети, ракети протиповітряної оборони "земля-земля" та надані Іраном дрони-камікадзе Shahed-136. Як повідомив 18 жовтня 2022 року Президент України, з 10 жовтня 30 % українських електростанцій було зруйновано, що спричинило масові вимкнення електроенергії по всій країні. Прес-служба Офісу Генпрокурора 24 жовтня повідомила, що з початку повномасштабного вторгнення російські військові здійснили 85 атак на об'єкти електроенергетики, з них 51 – у жовтні 2022 року. За таких умов саме підприємства паливно-енергетичного сектору стали цілями за результатами атак російських ракет й зазнали масштабних збитків. Терористичні удари по критичній інфраструктурі паливно-енергетичного сектору тривають у всіх регіонах України майже кожен день, що спричинює збитки, руйнування, сіяння паніки та страху.

Внаслідок масованих атак дронів на критичну інфраструктуру України протягом 2022 року, наслідками стали вихід із ладу та фізичне знищення окремих об'єктів енергетичної інфраструктури, тривалі аварійні відключення електропостачання. У зв'язку із цим кібербезпека сьогодні є життєво важливим фактором існування енергетичної галузі, надійний захист енергетичної системи від загроз у кіберпросторі [13].

Постановою Кабінету Міністрів України від 09.10.20 р. № 1109 "Деякі питання об'єктів критичної інфраструктури" [20] Міненерго визначено уповноваженим органом державної влади, відповідальним за паливно-енергетичний сектор критичної інфраструктури. Розробка секторальних (галузевих) вимог з кібербезпеки, наприклад, у паливно-енергетичного секторі передбачає підготовку відповідного наказу, що за наслідками його схвалення надасть змогу значно покращити стан кібербезпеки, підвищення захищеності інформаційних ресурсів та інформаційно-комунікаційних систем об'єктів критичної інфраструктури паливно-енергетичного сектору в цілому, до рівня, який забезпечує функціонування єдиного секторального (галузевого) безпечного інтегрованого інформаційного та комунікаційного середовища. Доцільно вказати, що, наприклад, існує Перелік об'єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури, затверджений наказом Міністерства енергетики України від 07.09.22 р. № 1-ДСК, зміст якого має обмежений доступ.

Методологія аналізу кіберзагроз та оцінки ризиків порушення кібербезпеки об'єктів енергетичної інфраструктури включає: поточний аналіз стану кіберзагроз об'єктів енергетичної інфраструктури, формування сценаріїв ймовірних екстремальних ситуацій, пов'язаних з реалізацією кіберзагроз, моделювання та оцінювання ризиків порушення кібербезпеки енергетичної інфраструктури. До переліку ризиків, які специфічні для підприємств енергетичної галузі, належать: використання в автоматизованих системах застарілого програмного забезпечення, обладнання та комунікаційних протоколів, які не передбачають можливості та вірогідності щодо кіберзагроз; наявність адміністративних та технологічних труднощів оновлення програмного забезпечення; неконтрольоване підключення автоматизованої системи управління до мережі Інтернет; можливий доступ "сторонніх" компаній до технологічної мережі об'єкта критичної інфраструктури [14, с. 116-117].

В цьому контексті необхідно якнайшвидше нарощувати потужності кіберзахисту об’єктів власної критичної інфраструктури, особливо щодо об’єктів критичної інфраструктури паливно-енергетичного сектору економіки. Поточні та майбутні чисельні атаки ворога саме на об’єкти критичної інфраструктури підтверджують тезу щодо необхідності такого посилення. Важливе місце на цьому фоні посідає секторальна кібербезпека та стандарти кібербезпеки в паливно-енергетичному секторі, удосконалення законодавства у цій площині.

Держава активно та постійно опікується питаннями посилення захисту об’єктів критичної інфраструктури. Повний перелік таких об’єктів ухвалює Уряд України, виходячи із таких критеріїв, як соціальна, політична, економічна значущість для забезпечення оборони країни та безпеки суспільства, рівень уразливості таких об’єктів.

Так, Постановою Кабінету Міністрів України від 16.12.22 р. № 1384 [23] викладено в новій редакції “Порядок віднесення об’єктів до критичної інфраструктури”, затверджений Постановою Уряду України від 09.10.20 р. № 1109. В оновленому форматі викладено механізми віднесення об’єктів до критичної інфраструктури та їх категоризації та визначено Перелік секторів (підсекторів), основних послуг критичної інфраструктури держави. Зокрема, до Переліку секторів критичної інфраструктури відносяться: паливно-енергетичний сектор, цифрові технології, захист інформації, харчова промисловість та агропромисловий комплекс, державний матеріальний резерв, охорона здоров’я, ринок капіталу та організованих товарних ринків, фінансовий сектор, транспорт і пошта, промисловість, сектор громадської безпеки, цивільний захист населення і територій, охорона навколишнього природного середовища, сектор оборони, національна безпека, правосуддя тощо. Загалом задекларовано, що відомості про об'єкти критичної інфраструктури, що містяться у зведеному переліку об’єктів критичної інфраструктури та секторальних переліках об’єктів критичної інфраструктури, є інформацією з обмеженим доступом, захист якої забезпечується відповідно до вимог законодавства.

Актуалізація питань забезпечення безпеки об’єктів критичної інфраструктури на державному рівні призвела до необхідності визначення уповноваженого та відповідального органу в сфері захисту критичної інфраструктури. Постановою Кабінету Міністрів України від 12.07.22 р. № 787 “Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості” [24] було утворено центральний орган виконавчої влади із спеціальним статусом, діяльність якого спрямовується і координується Урядом України. Цей орган забезпечує формування та реалізує державну політику у сфері захисту критичної інфраструктури та забезпечення національної системи стійкості. Враховуючи той факт, що інституційне становлення новоствореного державного органу потребує значного часу, 5 грудня 2022 року набув чинності Закон України № 2684-IX “Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України” [25]. Вказаний законодавчий акт було розроблено з метою належного забезпечення формування та реалізації державної політики у сфері критичної інфраструктури. Він спрямований на створення сприятливих передумов щодо виконання функцій уповноваженого органу з питань захисту критичної інфраструктури. Нормативно встановлено, що під час дії воєнного стану, а також протягом 12 місяців після його припинення чи скасування повноваження уповноваженого органу у сфері захисту критичної інфраструктури України, здійснюються саме Державною службою спеціального зв’язку та захисту інформації України.

Російські хакери здійснюють кожного дня у середньому понад десять кібератак на Україну. Це різні типи кібератак, іноді дійсно масові, іноді досить витончені. Цілі у них доволі різні: державні ресурси, об'єкти критичної інфраструктури тощо. Це вимагає від відповідальних державних та правоохоронних органів успішної системної протидії зухвалому та нахабному ворогу і в кіберпросторі. За таких умов держава має посилити захист об'єктів критичної інфраструктури від атак російських окупантів, забезпечити надійний стан захищеності об'єктів критичної інфраструктури (ОКІ), сприяти покращенню комплексної взаємодії операторів ОКІ та представників сектору безпеки і оборони України.

У рамках повноважень вітчизняні спецслужби розслідують кібератаки на об'єкти критичної інфраструктури України. Зокрема, діяльність Служби безпеки України зосереджена на контррозвідувальному, контртерористичному та протидиверсійному захисті об'єктів енергетики, транспортного комплексу, інших стратегічно важливих галузей. Саме вітчизняна спецслужба блокує та запобігає кібератакам ворога, використовуючи наявний власний потенціал та ресурси. Служба постійно блокує: спровоковані агресором нештатні й аварійні ситуації; перебої в роботі об'єктів життєдіяльності; маніпуляції у фінансово-банківському секторі; запобігає спробам знищити ліквідні і стратегічні підприємства. Серед пріоритетних завдань Служби безпеки України в галузі захисту ОКІ значна увага приділяється протидії іноземній економічній експансії, недопущенню використання фінансових інструментів для створення системних кризових явищ в українській економіці тощо [8, с. 157].

Так, у 2020 році СБУ зафіксувала 800 кібератак, у 2021 році – близько двох тисяч. Проте вже після повномасштабного вторгнення РФ в Україну їх зафіксували понад 4 500.Станом на 18 лютого 2023 року Служба безпеки України відбила понад 550 атак російських хакерів. Держава-агресор продовжує тримати темп і масованість в кібератаках, але абсолютну більшість українські спеціалісти зупиняють ще на початкових етапах. Найчастіше вони спрямовані на об'єкти логістики і транспорту, паливно-енергетичну галузь та військові об'єкти [26].

З метою посилення контрдиверсійного захисту об'єктів критичної інфраструктури спецслужба неодноразово проводила відповідні оперативні та контррозвідувальні заходи. Мета – посилення контрдиверсійного захисту об'єктів критичної інфраструктури та підвищення безпеки громадян в умовах російської збройної агресії проти України. Служба безпеки України також вживає контрдиверсійних заходів з метою нейтралізації загроз розвідувально-підривної діяльності проти державної безпеки України. До спільних профілактичних заходів залучаються на постійній основі підрозділи Нацполіції, Нацгвардії та Державної служби з надзвичайних ситуацій. Під посиленим захистом правоохоронців – стратегічно важливі об'єкти критичної інфраструктури та місця масового скупчення й перебування населення.

Як зазначає Голова Служби безпеки України, вітчизняна спецслужба в межах контрдиверсійних і антитерористичних заходів відстежує діяльність співробітників об'єктів критичної інфраструктури з метою виявлення серед них осіб, які можуть співпрацювати з РФ. Контррозвідувальним забезпеченням об'єктів критичної інфраструктури (зокрема, об'єктів енергетики) наразі успішно займається Головне управління "І" Служби безпеки України [27], діяльність якого дозволить інституційно-функціонально посилити, у тому числі, безпеку стратегічних галузей вітчизняної економіки в умовах правового режиму військового стану та триваючої кібервійни з державою-агресором.

Так, у січні 2023 року спецслужба викрила працівницю одного зі стратегічних об'єктів критичної інфраструктури Івано-Франківської області на виправдовуванні російської агресії та агітації за "руській мір". Уродженка Івано-Франківщини поширювала в соцмережі дописи, спрямовані на визнання правомірною збройної агресії російської федерації проти України. Під час обшуків за місцем проживання фігурантки СБУ вилучила комп'ютер та телефон з доказами протиправної діяльності. Фігурантці повідомлено про підозру за ч. 3 ст. 109 та ч. 3 ст. 436-2 КК України [27].

Також у січні 2023 року СБУ затримала російського агента, який "наводив" ворожі ракети на енергооб'єкти міста Одеса. Поплічник агресора збирав інформацію про розміщення підрозділів Сил оборони та об'єктів критичної інфраструктури на території регіону, намагався виявити бойові позиції української системи протиповітряної оборони, а також ворожого агента цікавили точні локації місцевих об'єктів енергетики. Зібрані відомості він зберігав на флешці, яку планував передати представнику російської спецслужби. За виконання злочинних завдань зрадник розраховував отримувати від ворога до 70 тис. грн. на місяць. Для збору розвідувальної інформації він виїжджав до різних районів Одеси та передмістя обласного центру, де здійснював фото- та відеофіксацію об'єктів. Під час обшуку у зловмисника виявлено флеш-носій із доказами підривної діяльності. На підставі зібраних доказів слідчі Служби безпеки повідомили фігуранту про підозру за ч. 2 ст.111 Кримінального кодексу України (державна зрада, вчинена в умовах воєнного стану)[28].

Крім цього, Служба безпеки України виявила мешканця Тернопільщини, який здавав ворогу розташування об'єктів енергетичної інфраструктури, працюючи на спецслужбу держави-агресора. Зрадник надавав ворогу інформацію про розташування та характеристики об'єктів критичної інфраструктури у Тернопільській області. Його було затримано оперативниками Служби безпеки України після того, як він отримав винагороду за зроблені знімки двох об'єктів енергетики у Тернополі й переслав ці фото куратору з ФСБ РФ. Затриманому оголосили підозру у державній зраді, скоєній в умовах воєнного стану[29].

Висновки.

Загальновідомо, що об'єкти критичної інфраструктури – це стратегічно важливі підприємства та установи, необхідні для функціонування суспільства країни та її економіки. Захист об'єктів критичної інфраструктури – комплексне та пріоритетне завдання держави в умовах сьогодення. В умовах війни з державою-агресором безпека об'єктів критичної інфраструктури здійснюється не тільки технічно, але й фізично. Існують загрозливі тенденції функціонування під постійними кібератаками ворога, об'єктів національної критичної інфраструктури, у першу чергу, паливно-енергетичного сектору. На цьому фоні актуального значення набувають питання впровадження секторальних вимог кібербезпеки щодо об'єктів критичної інфраструктури та проведення огляду стану кібербезпеки відповідних секторів економіки України. Це дозволить, у свою чергу, покращити стан кібербезпеки, підвищити захищеність інформаційних ресурсів та інформаційно-комунікаційних систем об'єктів критичної інфраструктури до рівня, який забезпечує функціонування єдиного секторального (галузевого) безпечного інтегрованого інформаційно-комунікаційного середовища. Питання посилення захисту об'єктів критичної інфраструктури енергетичної галузі від атак російських окупантів є гострим та важливим.

Держава робить важливі та поступальні кроки у напрямку посилення захисту об'єктів критичної інфраструктури. Зокрема, утворено новий державний орган – Державну службу захисту критичної інфраструктури та забезпечення національної

системи стійкості України, схвалено пакет законодавчих та нормативно-правових актів з метою врегулювання цієї сфери за стандартами НАТО та ЄС. Аналіз джерел законодавчого забезпечення захисту об'єктів критичної інфраструктури дає змогу констатувати, що протягом 2020 – 2022 років було схвалено низку нормативно-правових актів з метою врегулювання цієї сфери. Взагалі, виходячи із аналізу спеціального законодавства, присвяченого захисту об'єктів критичної інфраструктури, можна виокремити передові технологічні підходи, які практикуються в контексті розбудови захисту об'єктів критичної інфраструктури, зміст яких охоплює: організацію детекції незаконного порушення ліній периметра, сучасні можливості систем відео-аналітики на базі нейронних мереж, контроль доступу за допомогою безконтактної біоідентифікації, захист комп'ютерних систем для обробки таємної, службової та конфіденційної інформації, а також безперебійне живлення для комплексних систем безпеки тощо.

За наслідками повномасштабного вторгнення РФ в Україну у 2022 року кількість кібератак із боку РФ збільшилася вдвічі, а перед річницею воєнної агресії – у шість разів. Тобто у зв'язку зі збільшенням кількості та масштабів кібернападів як одного із проявів агресії Російської Федерації проти України набуває актуальності потреба вдосконалення нормативного забезпечення питань кіберзахисту інформаційних, електронних, комунікаційних й інформаційно-комунікаційних систем та об'єктів критичної інформаційної інфраструктури для здійснення ефективного стримування та протидії агресії проти України в кіберпросторі. За таких умов важливим напрямком посилення спроможностей держави у сфері забезпечення безпеки об'єктів критичної інфраструктури,особливо в умовах кібервійни, є прискорення прийняття законопроекту (реєстр. № 8087 від 29 вересня 2022 року) "Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури" [30].

Використана література

1. Бердецький Ю., Пальчик М. Окремі аспекти забезпечення кібербезпеки об'єктів критичної інфраструктури: досвід України. *Інформаційна безпека людини, суспільства, держави.* 2019. № 3(27). С. 49-56.
2. Ганкевич К.Б., Левчук В.Д., Корольов С.С. Особливості становлення правових засад існування об'єктів критичної інфраструктури України в системі Міністерства оборони України. *Юридичний науковий електронний журнал*. 2021. № 11. С. 79-82.
3. Іваненко О.І. Підхід до національної оцінки ризиків для критичної інфраструктури. *Вісник ХНТУ*. 2020. № 2(73). С. 9-22.
4. Кідалова Н.О. Правові проблеми захисту критичних об'єктів інфраструктури стратегічного значення в Україні. *Право. Людина. Довкілля.* 2019. № 3. С.124-131.
5. Ковалів М. Правове забезпечення кібербезпеки критичної інформаційної інфраструктури України / Р. Скриньовський, Ю. Назар, С. Єсімов, І. Красницький, Х. Кайдрович, С. Князь, Ю. Кемська. *Traektoriâ Nauki = Pathof Science*. 2021. Vol. 7. № 4. P. 2011-2018.
6. Когут Ю.І. Кібервійна та безпека об'єктів критичної інфраструктури: практичний посібник ; за ред. А.С. Довгопологого. Київ: Консалтингова компанія "СІДКОН", 2021. 332 с.
7. Кучерина С.Є, Олейніков Д.О. Сучасний стан кримінально-правової охорони об'єктів критичної інфраструктури. *Інформація і право.* № 1(36)/2021. С. 90-98.
8. Осипчук І.І. Правові засади діяльності Служби безпеки України як суб'єкта забезпечення критичної інфраструктури та місце серед них адміністративного законодавства. *Науковий вісник публічного та приватного права.* 2020. Т. 2. Вип. 6. С. 156-162.
9. Суходоля О.М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України. *Стратегічні пріоритети.* 2016. № 3. С. 62-76.

10. Павлов Д.М, Микитюк М.А. Правові та організаційні засади забезпечення захисту критичної інфраструктури у контексті формування нової безпекової парадигми України. *Честь і закон.* 2020. № 4 (75). С. 69-77.

11. Теленик С.С. Державна система захисту критичної інфраструктури України: концептуальні засади адміністративно-правового регулювання: монографія. Одеса: Видавничий дім "Гельветика". 2020. 602 с.

12. Цяпа С.М. Правове та організаційне забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак *Інформація і право.* № 4(39)/2021. С. 121-128.

13. Демедюк С. Кібербезпека сьогодні – життєво важливий фактор існування енергетичної галузі. URL: https://www.rnbo.gov.ua/ua/Diialnist/5024.html

14. Стежко С.М., Фіца В.М. Кібербезпека як важливий фактор забезпечення життєдіяльності вітчизняної енергетичної галузі. *Інформація і право.* № 4(39)/2021. С. 113-120.

15. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.21 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

16. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163. *Відомості Верховної Ради*. 2017. № 45. Ст. 403.

17. Про національну безпеку України: Закон України від 21.06.18 р. № 2469. *Відомості Верховної Ради*. 2018. № 31. Ст. 241.

18. Про критичну інфраструктуру: Закон України від 16.11.21 р. № 1882. URL: https://ips.ligazakon.net/document/T211882

19. Про затвердження Положення про організаційно-технічну модель кіберзахисту: Постанова Кабінету Міністрів України від 29.12.21 р. № 1426. URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennya-polozhennya-pro-a1426

20. Деякі питання об'єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 09.10.20 р. № 943.URL: https://zakon.rada.gov.ua/laws/show/943-2020-п#Text

21. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом: Постанова Кабінету Міністрів України від 11.11.20 р. № 1176. URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennya-poryadku-prove-a1176

22. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.19 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text

23.Про внесення змін до Постанови Кабінету Міністрів України від 09.10.20 р. № 1109: Постанова Кабінету Міністрів України від 16.12.22 р. № 1384. URL: https://www.kmu.gov.ua/npas/pro-vnesennia-zmin-do-postanovy-kabinetu-ministriv-ukrainy-vid-9-zhovtnia-2020-r-1109-1384-161222

24. Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості: постанова Кабінету Міністрів України від 12.07.22 р. № 787.URL: https://www.kmu.gov.ua/npas/pro-utvorennia-derzhavnoi-sluzhby-zakhystu-krytychnoi-infrastruktury-ta-zabezpechennia-natsionalnoi-systemy-stiikosti-uk

25.Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України: Закон України від 18.10.22 р. № 2684. URL: https://ips.ligazakon.net/document/t222684?an=

26. Цього року СБУ уже нейтралізувала понад 500 російських кібератак. URL: https://www.slovoidilo.ua/2023/02/18/novyna/bezpeka/czoho-roku-sbu-uzhe-nejtralizuvala-500-rosijskyx-kiberatak

27. На Івано-Франківщині працівниця об'єкта критичної інфраструктури агітувала за "руській мір".URL: sivnitsya-ob-yekta-kritichnoyi-infrastrukturi-agituvala-za-ruskiy-mir

28. Збирав інформацію про місцерозташування ППО та критичної інфраструктури: СБУ затримала агента ФСБ в Одесі. URL: https://ssu.gov.ua/novyny/sbu-zatrymala-rosiiskoho-ahenta-yakyi-navodyv-vorozhi-rakety-na-enerhoobiekty-odesy

29. Зливав ворогу дані про підстанції на заході України: СБУ затримала 20-річного зрадника. URL: https://www.pravda.com.ua/news/2023/01/30/7387127

30. Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури: проект Закону України від 29 вересня 2022 року № 8087. URL: https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=8087&conv=9

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~