УДК 342.951

АРПЕНТІЙ С.П., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0003-3326-3942.

ШЛЯХИ УДОСКОНАЛЕННЯ ЗАКОНОДАВЧОГО ЗАБЕЗПЕЧЕННЯ ОРГАНІЗАЦІЙНО-ТЕХНІЧНОЇ МОДЕЛІ КІБЕРЗАХИСТУ В УМОВАХ РОСІЙСЬКОЇ ВІЙСЬКОВОЇ АГРЕСІЇ

Анотація. *Визначено роль та місце організаційно-технічної моделі кіберзахисту як важливої складової національної системи кібербезпеки. Обґрунтовано мету та завдання організаційно-технічної моделі кіберзахисту в умовах російської військової агресії. Проведено аналіз нормативно-правових актів, присвячених регламентації питань щодо особливостей розвитку та впровадження організаційно-технічної моделі кіберзахисту. Деталізовано заходи, які здійснювалися з метою розбудови організаційно-технічної моделі кіберзахисту. Розкрито зміст та особливості практичного впровадження організаційно-технічної моделі кіберзахисту в умовах війни. Проведено огляд вітчизняного законодавства, присвяченого розбудові організаційно-технічної моделі кіберзахисту. Узагальнено подальші шляхи удосконалення нормативного забезпечення процесів розвитку організаційно-технічної моделі кіберзахисту в умовах поширення кіберзагроз.*

Ключові слова: *національна система кібербезпеки, організаційно-технічна модель кіберзахисту, кіберінцидент, кіберзагроза, кібердомен, кіберпростір, російська військова агресія, правовий режим воєнного стану, державна кібербезпекова політика, критична інфраструктура.*

Summary. *The role and place of the organizational and technical model of cyber protection as an important component of the national cyber security system is determined. The purpose and tasks of the organizational and technical model of cyber protection in the conditions of Russian military aggression are substantiated. The analysis of regulatory legal acts devoted to the regulation of issues regarding the specifics of the development and implementation of the organizational and technical model of cyber protection was carried out. The measures taken to develop the organizational and technical model of cyber protection are detailed. The content and features of the practical implementation of the organizational and technical model of cyber protection in war conditions are disclosed. A review of domestic legislation dedicated to the development of the organizational and technical model of cyber protection was conducted. Further directions of improving the regulatory support of the development processes of the organizational and technical model of cyber protection in the conditions of the spread of cyber threats are summarized.*

Keywords: *national cyber security system, organizational and technical model of cyber protection, cyber incident, cyber threat, cyber domain, cyber space, Russian military aggression, legal regime of martial law, state cyber security policy, critical infrastructure.*

Постановка проблеми. Кіберпростір являє собою новий канал для створення і поширення різноманітної інформації, стаючи новим двигуном зростання цифрової економіки, новою платформою соціального управління, новим способом міжнародного співробітництва, до того ж і зовсім новою сферою державного суверенітету. Однак кіберпростір надає не тільки ресурси, можливості, але і містить певні загрози. Посилена цифровізація та зв'язок збільшують ризики кібербезпеки, тим самим роблячи суспільство загалом більш вразливим до кіберзагроз, посилюючи небезпеку.

З метою зменшення цих ризиків світова спільнота опікується питаннями розробки та вжиття всіх необхідних заходів щодо поліпшення стану кібербезпеки. Одночасно підвищення ефективності функціонування національної системи кібербезпеки є основним завданням для забезпечення сталого і безпечного функціонування держави та національної критичної інформаційної інфраструктури в кіберпросторі. Військово-політичне керівництво провідних держав світу визнає протиборство в кіберпросторі як одну із вирішальних умов реалізації національних інтересів і вигідного врегулювання кризових ситуацій.

З урахуванням вирішення цієї задачі розвиваються національні та міждержавні органи управління, сили та засоби кібервійн, реалізуються нові підходи до побудови системи протиборства в кіберпросторі на всіх рівнях. Кіберзагрози у сучасному світі набувають значного масштабу. Відтепер успішна атака хакерів може знеструмити цілу область або країну, а кіберзагрози являють собою наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави та її об'єктів. За таких умов посиленому кіберзахисту підлягає як система накопичення інформації, так і сама інформаційна система, оскільки уразливими для реалізації кіберзагроз є об'єкти, функціонування комп'ютерних систем яких пов'язане з використанням ресурсів кіберпростору.

Одним із напрямів забезпечення функціонування національної системи кібербезпеки є впровадження її організаційно-технічної моделі. З набуттям чинності Законом України "Про основні засади забезпечення кібербезпеки України" [1] ще у травні 2018 року перед державою постало актуальне та важливе завдання щодо визначення та деталізації подальших кроків розбудови національної системи кібербезпеки. Протягом останніх років з метою посилення національної системи кібербезпеки розроблявся сценарій та визначалися практичні аспекти створення та запровадження вітчизняної організаційно-технічної моделі кіберзахисту. Стратегія кібербезпеки України [2], схвалена у 2021 році, чітко декларує, що однією із передумов та чинників, які формують загрози кібербезпеці України є незавершеність заходів із впровадження організаційно-технічної моделі кіберзахисту, яка має відповідати сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки. Тобто важливим завданням державної кібербезпекової політики, особливо в умовах правового режиму воєнного стану, вбачається забезпечення динамічного розвитку вітчизняної організаційно-технічної моделі кіберзахисту. Цей процес було значно пришвидшено в умовах особливого періоду, що пов`язано із російською військовою агресією, у тому числі й в кібердомені. Законодавчо визначено, що функціонування національної системи кібербезпеки забезпечується шляхом впровадження організаційно-технічної моделі кіберзахисту як комплексу заходів, сил і засобів, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем. В умовах повномасштабної російської військової агресії проти України розвиток складових національної системи кібербезпеки і, в першу чергу, організаційно-технічної моделі кіберзахисту набуває актуальності та потребує деталізації на науково-практичному рівні.

Результати аналізу наукових публікацій. Національна система кібербезпеки та її складові стали предметом підвищеної уваги таких науковців, як: І. Діордиці [3], А. Марущака та С. Петрова [4], А. Тарасюка [5]. Подальші шляхи посилення стану забезпечення кібербезпеки конкретизували у своїх наукових працях: С. Красніков [6],

Ю. Яковенко та Ю. Деркаченко [7]. Питання розвитку складових організаційно-технічної моделі кіберзахисту та її архітектури вивчали у своїх працях: Я. Мануілов [8], В. Голь, А. Раківська та Д. Раківський [9], А. Омельченко [10]. Проте жоден із вказаних фахівців та експертів предметно не досліджував особливості та подальші шляхи удосконалення законодавчого забезпечення організаційно-технічної моделі кіберзахисту в умовах російської військової агресії. Ці обставини свідчать про актуальність тематики цієї наукової статті.

Метою статті є визначення, на підставі проведеного аналізу, пріоритетних засад державної кібербезпекової політики та огляду вітчизняного законодавства перспективних шляхів удосконалення правового забезпечення організаційно-технічної моделі кіберзахисту як важливої складової національної системи кібербезпеки в умовах правового режиму воєнного стану.

Виклад основного матеріалу. Починаючи з 24 лютого 2022 року Україна залишається на першому місці у світі за кількістю кібератак проти неї. Якщо класифікувати кібератаки на три основні групи, то до першої можна віднести операції інформаційного впливу, які теж реалізуються через кібератаки (наприклад, через злам медіа або веб-ресурсів офіційних органів). Друга група – це кібершпигунство для отримання інформації. І третя – це операції ефекту, тобто деструктивні кібероперації, внаслідок яких знищують дані, інфраструктуру тощо. Це, наприклад, атаки на телеком-провайдерів, онлайн-сервіси, зокрема й державні. Серед всіх російських угрупувань, відповідальних за кіберагресію, є три групи, які можна класифікувати. Перша – це військові хакери – співробітники спецслужб: фсб, служби зовнішньої розвідки, ГУ ГШ ЗС рф, інститутів міністерства оборони Це відомі угруповання "Sandworm", "APT28", "Armageddon" у складі фсб, "APT29", яке асоціюється зі службою зовнішньої розвідки рф. Це найнебезпечніші та найбільш підготовлені, найкраще забезпечені фінансово хакери. Друга група – кіберзлочинці, тобто ті, хто обкрадає фінансові установи, банки, криптогаманці. Це "чистий кіберкримінал", якого в росії було завжди багато. Третя група – це так звані хактивісти, які прагнуть через кібератаки досягти певних військово-політичних цілей. Вони збираються у групи через закриті канали в мережі "Telegram", та у кожній такій групі є куратор – офіцер фсб або гру, який спрямовує їхню діяльність. Адже їм ставлять завдання, досягнення яких передбачає отримання грошової винагороди. Це все – складові державної російської машини, політика якої – тероризм, у тому числі глобальний кібертероризм.

З метою запобігання вказаним викликам та загрозам у кібердомені, основні суб'єкти національної системи кібербезпеки ведуть роботу за кількома стратегічними напрямами – посилення кіберзахисту та організація фізичного захисту даних, критичної інфраструктури, інформаційно-комунікаційних систем для чого активно використовується організаційно-технічна модель кіберзахисту, яка являє собою комплекс заходів, сил і засобів, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем. Застосування цієї моделі має на меті об'єднати зусилля суб'єктів забезпечення кібербезпеки та створити належні сприятливі передумови для безпечного функціонування кіберпростору (кібердомену), його використання в інтересах особи, суспільства і держави, зокрема через реалізацію заходів, спрямованих на захист національних інформаційних ресурсів, посиленого кіберзахисту об'єктів критичної інформаційної інфраструктури, забезпечення їх кіберстійкості, стабільного функціонування інформаційної інфраструктури державного та приватного секторів економіки. Таким чином, організаційно-технічна модель

кіберзахисту спрямована на створення передумов з метою об'єднання зусиль та потенціалу суб'єктів забезпечення кібербезпеки задля вирішення завдання підвищення рівня кіберстійкості критичної інформаційної інфраструктури держави, яка охоплює як об'єкти критичної інфраструктури, комунікаційно-інформаційні та інші системи, сталість та надійність функціонування яких критично важлива для функціонування державних органів, підприємств, установ і організацій всіх форм власності.

З метою реагування на кіберзагрози та враховуючи актуальність та своєчасність необхідності розробки і запровадження власної організаційно-технічної моделі кіберзахисту Кабінет Міністрів України 29 грудня 2021 року затвердив положення про організаційно-технічну модель кіберзахисту [11]. Основним завданням схвалення зазначеного нормативно-правового акту стала необхідність забезпечення безперебійного функціонування національної системи кібербезпеки держави. У свою чергу, організаційно-технічна модель кіберзахисту спрямована на забезпечення: функціонування системи кіберзахисту України та посилення координації дій між основними суб'єктами кібербезпеки; зменшення вразливості інформаційних, комунікаційних систем і забезпечення їх кіберстійкості; створення передумов для розвитку державно-приватного партнерства у сфері кібербезпеки та ефективної системи національного реагування на кіберінциденти, зокрема – розвиток галузевих команд реагування, синхронізація та узгодження їхніх дій; підвищення національного потенціалу в галузі кібербезпеки у кіберпросторі; запровадження постійного контролю за станом кіберзахисту об'єктів критичної інфраструктури; конфіденційності, цілісності та доступності інформації, а також безпеки комунікаційних і технологічних систем.

Одночасне впровадження організаційно-технічної моделі кіберзахисту визначає сферу відповідальності за виконання конкретних завдань кожного суб'єкта кібербезпеки та надає можливість сформувати ефективну систему ресурсного забезпечення, у тому числі кадрів. Нормативно встановлено, що функціонування організаційно-технічної моделі кіберзахисту забезпечується шляхом: формування та реалізації державної політики у сфері кібербезпеки, зокрема з урахуванням досвіду держав-членів ЄС та НАТО; координації суб'єктів кіберзахисту під час здійснення заходів щодо забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури та національних електронних інформаційних ресурсів; кіберзахисту інформаційно-телекомунікаційних систем, що обробляють національні електронні інформаційні ресурси, комунікаційних систем та об'єктів критичної інформаційної інфраструктури, їх кіберстійкості, здійснення постійного контролю за станом їх кіберзахисту; розвитку системи реагування на кіберзагрози; розвитку сил кіберзахисту та системи їх координації; створення систем управління ризиками інформаційної безпеки на об'єктах критичної інфраструктури; формування та розвитку спроможностей суб'єктів забезпечення кібербезпеки; створення умов для безпечного функціонування інформаційної інфраструктури державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до закону, підприємств, установ та організацій незалежно від форми власності; створення умов для розвитку державно-приватної взаємодії в сфері кібербезпеки; розвитку системи кадрового, матеріально-технічного та експертно-аналітичного забезпечення сил кіберзахисту; розвитку та постійного вдосконалення систем кіберзахисту об'єктів критичної інфраструктури з урахуванням результатів оцінки повноти, адекватності, результативності та ефективності процесів, що виконуються в рамках впровадження системи інформаційної безпеки на об'єктах критичної інфраструктури.

Дієвими засобами кіберзахисту, які використовуються з метою впровадження організаційно-технічної моделі кіберзахисту, є системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, інформаційні технології, технічні і програмні засоби (пристрої, обладнання, комплекси), які використовуються в інтересах забезпечення кіберзахисту національних електронних інформаційних ресурсів, комунікаційних і технологічних систем, а також об'єктів критичної інформаційної інфраструктури. У свою чергу, в процесі практичного впровадження організаційно-технічної моделі кіберзахисту застосовуються організаційно-правові, інженерно-технічні заходи та заходи з криптографічного та технічного захисту інформації, які проводяться силами кіберзахисту та базуються на принципах персональної відповідальності за власні дії та колективної відповідальності за безпеку кожного, забезпечення пропорційності та співрозмірності заходів реальним та потенційним ризикам.

Організаційно-технічна модель кіберзахисту передбачає три рівні інтегрованих інфраструктур кіберзахисту: 1) організаційно-керівна (основні суб'єкти національної системи кібербезпеки); 2) технологічна (взаємодія технологічних підрозділів, тобто обмін інформацією, моніторинг, забезпечення сталої безпеки кіберпростору тощо); 3) базова (захищена інформаційна інфраструктура та суспільство (громада). Практична реалізація заходів із кіберзахисту відповідними системами передбачає компонування таких процесів, як: *ідентифікацію* – виявлення реальних і потенційних кіберзагроз для запобігання їм 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, мінімізації їх можливих наслідків (запобігання виникненню загроз життю або здоров'ю людей та заподіяння шкоди майну), удосконалення систем кіберзахисту, з урахуванням необхідності забезпечення пропорційності або співрозмірності можливостей таких систем реальним та потенційним ризикам; *відновлення* – поновлення штатного режиму функціонування інформаційно-телекомунікаційних та технологічних систем після кібератаки, відновлення інформації і відомостей у разі їх пошкодження або видалення, створення передумов щодо проведення розслідування за наслідками кібератак. Схвалення цієї постанови має на меті врегулювання питань щодо практичного впровадження організаційно-технічної моделі кіберзахисту, визначення її мети, архітектури, складу, основних напрямів діяльності суб'єктів забезпечення кібербезпеки, які реалізовують заходи в межах забезпечення функціонування національної системи кібербезпеки.

Нормативно-правове визначення організаційно-технічної моделі кіберзахисту надасть можливість здійснювати її розвиток планово, на підставі збалансованих та обґрунтованих рішень, які будуть спрямовуватись на врегулювання прогалин у нормативно-правовому регулюванні, розробці процедур взаємодії суб'єктів забезпечення кібербезпеки України, впровадження ризик-орієнтованого підходу до прийняття рішень в сфері кібербезпеки, розвитку механізмів державно-приватної взаємодії, зміцнення довіри між державним та приватним сектором на основі прозорих та взаємовигідних процедур обміну інформації [12, с. 58].

У рамках розбудови організаційно-технічної моделі кіберзахисту 22 вересня 2022 року на засіданні Національного координаційного центру кібербезпеки РНБО України було схвалено Порядок взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки [13]. Передбачається, що під час взаємодії

створення постійної об'єднаної групи реагування на кіберінциденти та кібератаки та врегульовано питання інформаційного обміну, координації та спільних дій суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки. Залежно від ступеня негативних наслідків, що можуть настати в результаті реалізації кіберінциденту/кібератаки, запроваджується шість рівнів критичності, які були розроблені з урахуванням кращих світових практик: некритичний (білий), низький (зелений), середній (жовтий), високий (помаранчевий), критичний (червоний) та надзвичайний (чорний). Відповідно до рівня критичності документом визначені алгоритми взаємодії під час реагування на загрози.

Важливим напрямком функціонування організаційно-технічної моделі кіберзахисту є налагодження оперативного обміну інформацією про кіберінциденти. Так, рішенням Національного координаційного центру кібербезпеки при Раді національної безпеки та оборони України (протокол №21 засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України від 9 лютого 2023 року) були затверджені Загальні правила обміну інформацією про кіберінциденти (Протокол TLP) [14]. Ці Правила є обов'язковими для використання основними суб'єктами національної системи кібербезпеки, іншими державними органами, зокрема секторальними органами у сфері захисту критичної інфраструктури, а також рекомендованими для об'єктів критичної інфраструктури під час формування повідомлень про кіберінциденти. Одночасно такі Правила не призначені для позначення інформації, що становить державну, банківську таємницю та службову інформацію.

Задля реалізації та практичного впровадження організаційно-технічної моделі кіберзахисту Кабінет Міністрів України своєю постановою "Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі" від 4 квітня 2023 року [15] визначив порядок та процедури реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі. Зокрема реагування на кіберінциденти/кібератаки здійснюється суб'єктами забезпечення кібербезпеки послідовно такими етапами, як: підготовка, виявлення та аналіз, стримування, усунення, відновлення, аналіз ефективності заходів з реагування на кіберінциденти/кібератаки. Задекларовано, що кожен суб'єкт забезпечення кібербезпеки за результатами кінцевого вжиття заходів у сфері кіберзахисту проводить аналіз ефективності реагування на кіберінциденти або кібератаки, вивчає задокументовані дані щодо кіберінцидентів або кібератак, здійснює відповідне інформування керівництва суб'єкта забезпечення кібербезпеки, проводить аналіз досвіду реагування для подальшого підвищення ефективності вжиття заходів кіберзахисту у разі можливих кіберінцидентів або кібератак у подальшому. В контексті викладеного важливим залишається організація та забезпечення кіберзахисту державних електронних інформаційних ресурсів та критичної інформаційної інфраструктури, що передбачає впровадження організаційно-технічної моделі національної системи кібербезпеки, а також оперативне реагування на кібератаки та кіберінциденти.

З метою забезпечення розвитку складових організаційно-технічної моделі кіберзахисту Уряд України своєю постановою затвердив Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури [16]. Розроблений за ініціативою Адміністрації Держспецзв'язку вказаний нормативний акт визначає стратегічні цілі, заходи, завдання для суб'єктів національної системи захисту критичної інфраструктури (далі – КІ), секторальних органів, операторів КІ та інших державних органів. Національний план – це дорожня карта, відповідно до якої має відбуватися планування в галузі захисту критичної інфраструктури. Так, зокрема Національний план

передбачає: уточнення завдань та повноважень суб'єктів захисту критичної інфраструктури, удосконалення законодавства, що регламентує їхню діяльність; забезпечення проведення моніторингу; проведення оцінки ризиків і загроз критичній інфраструктурі; визначення порядку взаємодії суб'єктів захисту КІ у кризових ситуаціях; забезпечення функціонування системи обміну інформацією; посилення стійкості КІ; розроблення програм щодо роботи з громадами та підтримки населення на випадок кризових ситуацій; налагодження міжнародної співпраці тощо. Виконання Національного плану, який розрахований на три роки, сприятиме безперебійній роботі об'єктів критичної інфраструктури різних категорій, забезпечить захист від загроз та безперебійне надання життєво важливих послуг населенню, має посилити організаційно-технічну модель кіберзахисту. Згідно з положеннями Національного плану місцеві органи виконавчої влади (військово-цивільні адміністрації) мають розробити та затвердити місцеві програми забезпечення безпеки та стійкості критичної інфраструктури, програми підвищення стійкості територіальних громад до кризових ситуацій, викликаних припиненням або погіршенням надання важливих для їх життєдіяльності послуг чи для здійснення життєво важливих функцій.

Оскільки організаційно-технічна модель кіберзахисту є важливою складовою національної системи кібербезпеки, то відповідно до п. 38 Плану заходів на 2023 – 2024 роки з реалізації Стратегії кібербезпеки України, затвердженого Розпорядженням Кабінету Міністрів України від 19.12.23 р. № 1163 [17], передбачається забезпечення її розвитку шляхом розроблення відповідного переліку нормативно-правових актів, присвячених цій тематиці і одночасне визначення необхідних заходів та відповідальних суб'єктів, які мають забезпечувати розвиток структурних елементів організаційно-технічної моделі кіберзахисту в різних інфраструктурах. Ключовими напрямами відповідно до зазначеного плану мають стати: нормативно-правове забезпечення діяльності у сфері кібербезпеки, кіберзахисту та кібероборони; розвиток технологічної складової національної системи кібербезпеки та організаційно-технічної моделі кіберзахисту.

Таким чином, організаційно-технічна модель як важлива складова національної системи кібербезпеки, передбачає, передусім, забезпечення безперебійного функціонування автоматизованих систем органів військового та державного управління, оскільки в сучасних умовах з метою ефективного відбиття кібератак та гарантування надійного кіберзахисту вказані системи повинні вдосконалюватися в напрямі підвищення ступеня їх автоматизації та комп'ютеризації. Враховуючи викладене, актуальною та сучасною вимогою сьогодення є перегляд принципів побудови автоматизованих систем органів військового та державного управління кібербезпекою як у мирний, так і у воєнний час. В контексті розбудови національної системи кібербезпеки важливим напрямком залишається перспективне використання її інтелектуальної підсистеми. Саме інтелектуальна підсистема кібербезпеки надасть можливість не тільки оперативно виявляти нові, невідомі та нетипові кібератаки в процесі моніторингу кіберпростору, але й системно аналізувати виявлені кіберзагрози й автоматично обирати параметри функціонування автоматизованих систем в умовах деструктивних впливів без погіршення їх основних характеристик.

З цього приводу О. Бакалинський та Д. Пахольченко обґрунтовано вважають, що вкрай необхідним є прискорення процесу імплементації міжнародних стандартів та розробка власних стандартів, нормативно-правових документів з урахуванням міжнародних вимог, передусім, – стандартів з кібербезпеки технологічних систем, зважаючи на їх вплив на кіберстійкість критичної інфраструктури [18, с. 109].

У рамках розбудови організаційно-технічної моделі кіберзахисту, окрім вдосконалення складових функціонування автоматизованих систем органів військового та державного управління, також мають бути реалізовані можливості щодо: автоматичної зміни властивостей та параметрів підсистем і засобів забезпечення кібербезпеки залежно від зміни стану кіберпростору (виявлення активності потенційних джерел кіберзагроз, виявлення кібератак) та результатів проведених кібератак; автоматичної оцінки змін захищеності автоматизованих систем органів військового та державного управління від кіберзагроз при диференційованих умовах функціонування; автоматизованої підтримки прийняття рішень щодо протидії кібератакам та автоматичного впливу на джерело кібератаки; автоматизованої підтримки прийняття рішень щодо перерозподілу ресурсів систем та засобів забезпечення кібербезпеки на випадок їх функціонального ураження в результаті кібератак; обліку у процесі посилення кібербезпеки всіх взаємопов'язаних та взаємодіючих факторів, які можуть впливати на рівень її забезпечення; контролю та зниження нецільового навантаження на комплекси засобів автоматизації систем кібербезпеки; прогнозування на підставі отриманих у процесі експлуатації програмно-апаратних комплексів знань та факторів, що можуть впливати на рівень захищеності автоматичних систем управління від усіх видів кіберзагроз.

Таким чином, основою організаційно-технічної моделі кіберзахисту є система функціонування автоматизованих систем органів військового та державного управління, яка включає такі складові: постійний моніторинг кіберпростору, комплексний захист інформації, оперативне оповіщення про кібератаки або кіберзагрози та протистояння їм; запровадження єдиних стандартів управління кібербезпекою; конструктивну взаємодію суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки. Під час дії воєнного стану та протягом 12 місяців після його припинення чи скасування уповноваженим органом у сфері захисту критичної інфраструктури України та перспективної розбудови організаційно-технічної моделі кіберзахисту визначено саме Держспецзв'язку, до повноважень якого віднесено координацію діяльності суб'єктів національної системи захисту, забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури.

Висновки.

Україна – одна з небагатьох країн світу, в яких на державному рівні закріплені правила взаємодії різних державних органів та структур для забезпечення кіберзахисту в контексті організаційно-технічної моделі кіберзахисту. Одночасно ця модель кіберзахисту формує передумови щодо мінімізації ймовірних негативних наслідків для інформаційно-комунікаційних систем. Практичне її впровадження також визначає сфери відповідальності за виконання конкретних завдань кожного суб'єкта кібербезпеки та надає можливість сформувати ефективну систему відповідного ресурсного забезпечення. При цьому, ця модель визначає завдання із забезпечення кіберзахисту на усіх можливих рівнях. Таким чином, організаційно-технічна модель кіберзахисту – це важлива складова національної системи кібербезпеки. Механізми імплементації цієї моделі та її ресурсне забезпечення – два важливі компоненти, які охоплюють всі рівні архітектури кібербезпеки. Механізми імплементації – це розробка і удосконалення нормативно-правової бази шляхом прийняття відповідних законодавчих актів, стандартів, локальних актів на всіх рівнях управління кібербезпекою. Можна констатувати успішний досвід останніх років щодо розбудови вітчизняної організаційно-технічної моделі. Так, зокрема у рамках реалізації державної кібербезпекової політики за ініціативи Адміністрації Держспецзв'язку зроблено важливі

та поступальні кроки з метою розвитку вітчизняної Організаційно-технічної моделі кіберзахисту.

До важливих здобутків на державному рівні протягом 2021 – 2023 років слід віднести: нормативне схвалення створення організаційно-технічної моделі кіберзахисту; розробка загальних правил обміну інформацією про кіберінциденти (протокол TLP) тощо. Практичний аспект впровадження сучасної організаційно-технічної моделі кіберзахисту очікувано сприятиме посиленню координації діяльності складових сектору безпеки і оборони України, їхньої техніко-технологічні можливості в рамках цілісної управлінської системи щодо протидії та профілактики боротьби з російськими та іншими кіберзагрозами незалежно від способу, мети та суб'єкта їх реалізації.

Таким чином, узагальнюючи викладене можна дійти висновку, що організаційно-технічна модель кіберзахисту не тільки окреслює комплексні межі (Framework) і різні рівні інфраструктури захисту країни в кіберпросторі, але й на підзаконному рівні визначає основні етапи та стадії реагування на кіберінциденти та кіберзагрози. Такий комплексний підхід має підвищити ефективність національної системи кібербезпеки, що, зокрема, дозволить державному та приватному секторам розробляти, впроваджувати та постійно удосконалювати структурно однакові та адаптовані під власні потреби планові заходи реагування на кіберінциденти та кібератаки.

Використана література

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. 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://zakon.rada.gov.ua/laws/show/447/2021#Text

3. Діордиця І.В. Адміністративно-правове регулювання кібербезпеки України: автореф. дис. …д-ра юрид. наук: спец. 12.00.07. Запоріжжя, 2018. 40 с.

4. Марущак А.І., Петров С.Г. Сучасний стан розвитку національної системи кібербезпеки (на прикладі СБ україни та Держспецзв'язку України). *Інформація і право.* № 2(33)/2020. С. 77-84.

5. Тарасюк А.В. Пріоритети правового забезпечення кібербезпеки в Україні на сучасному етапі. *Прикарпатський юридчний вісник.* 2020. Вип. № 1. С. 133-136.

6. Красінков С.А. Шляхи посилення стану забезпечення кібербезпеки в умовах воєнного стану. *Інформація і право.* № 3(46)/2023. С. 118-128.

7. Яковенко Ю.Л., Деркаченко Ю.В., Кухтик С.В., Березовський Д.О. Шляхи удосконалення системи кібербезпеки в Україні. *Проблеми сучасних трансформацій. Серія: Право, публічне управління та адміністрування.* 2021. № 1. Вип. І. С. 87-93.

8. Мануілов Я.С. Щодо концепції організаційно-технічної моделі кіберзахисту. *Інформація і право.* № 2(37)/2021. С. 115-122.

9. Голь В.Д., Раківська А.Ю., Раківський Д.Ю. Засоби кіберзахисту на рівні мережної інфраструктури. *Системи управління, навігації та зв`язку.* 2022. Вип. 3 (69). С. 116-120.

10. Омельченко А.В. Організаційно-правові засади забезпечення кібербезпеки України. 2021. *Київський часопис права.* 2021. № 3. С. 140-145.

11. Про затвердження Положення про організаційно-технічну модель кіберзахисту: Постанова Кабінету Міністрів України від 29.12.21 р. № 1426. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text

12. Потій О., Семенченко А., Бакалинський О., Мялковський Д. Концептуальні засади впровадження організаційно-технічної моделі кіберзахисту України. *Захист інформації.* 2021. Т. 23. № 1. С. 47-60.

13. Порядок взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки. – (Одноголосно затверджено на засіданні НКЦК). URL: https://www.rnbo.gov.ua/ua/Diialnist/5765.html

14. Загальні правила обміну інформацією про кіберінциденти (Протокол TLP): URL: https://cert.gov.ua/recommendation/4256181

15. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Постанова Кабінету Міністрів України від 04.04.23 р. № 299. URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text

16. Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури: Розпорядження Кабінету Міністрів України від 19.09.23 р. № 825. URL: https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text

17. Про затвердження плану заходів на 2023 – 2024 роки з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 19.12.23 р. № 1163. URL: https://zakon. rada.gov.ua/laws/show/1163-2023-%D1%80#Text.

18. Бакалинський О.О., Пахольченко Д.В. Аналіз вимог до кіберзахисту автоматизованих систем управління технологічними процесами як об'єктів критичної інформаційної інфраструктури. *Електронне моделювання.* 2021. Т. 43. № 4. С. 103-112.

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