**Вступ**

Постановою Кабінету Міністрів України від 29 грудня 2021 р.   
№ 1426 затверджено [Положення про організаційно-технічну модель кіберзахисту](https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text).

**Цілі прийняття акта Уряду.** [*Закон України «Про основні засади забезпечення кібербезпеки України»*](https://zakon.rada.gov.ua/laws/show/2163-19#n109) визначає правові та організаційні основи забезпечення захисту в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, національну систему кібербезпеки, повноваження суб’єктів забезпечення кібербезпеки та засади координації.

Одним із визначених Законом напрямів забезпечення функціонування національної системи кібербезпеки є впровадження її організаційно-технічної моделі. Організаційно-технічна модель кіберзахисту (ОТМ) розроблена фахівцями Держспецзв'язку, ґрунтуючись на п’ятирічній практиці застосування норм та положень цього Закону, досвіді розбудови національної системи кібербезпеки, аналізі сильних та слабких сторін моделей кібербезпеки інших країн, практиці організації роботи у цій сфері та взаємодії з іншими суб’єктами забезпечення кібербезпеки.

Положення про ОТМ визначає саму модель, її місію, склад та структуру, механізм функціонування та цілі. Вперше визначені дефініції сил та засобів кіберзахисту, команд реагування на комп‘ютерні надзвичайні події, кібергігієни. ОТМ передбачає багаторівневу архітектуру, яка являє собою структуровану систему, що складається з трьох інфраструктур, кожна з яких охоплює відповідні сектори, рівні та елементи.

Верхній рівень – організаційно-керуюча інфраструктура – сукупність суб’єктів забезпечення кібербезпеки, що формують та/або реалізують державну політику у сфері кібербезпеки; середній рівень – технологічна інфраструктура – сукупність сил та засобів кіберзахисту та їх забезпечення; та базовий рівень – базисна інфраструктура – сукупність об’єктів критичної інформаційної інфраструктури та їх критичних активів, суб’єктів господарювання, громадян України та об’єднань громадян, інших осіб, які провадять діяльність та/або надають відповідні послуги.

Положенням про ОТМ визначено, що її впровадження спрямоване на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів та мінімізацію вразливості комунікаційних систем.

Положення про ОТМ окреслює цілісну, не суперечливу, об‘єднану єдиним задумом структуровану систему, місце в ній кожного суб’єкта національної системи кібербезпеки, характер зв’язків з іншими суб‘єктами, форми взаємодії між різними суб’єктами одного та інших рівнів моделі, напрями інформаційного обміну, основні етапи управління кіберінцидентами та базові механізми запобігання, виявлення, ідентифікації, реагування на кіберінциденти і кібератаки та відновлення після них. Положення про ОТМ чітко сформульовало екосистему кібербезпеки, в якій всі її учасники тісно пов’язані між собою, доповнюють діяльність один одного, а характер відносин є здебільшого партнерським, а не адміністративно-командним.

*Положення про ОТМ розроблено на виконання* [*частини третьої статті 8 Закону України «Про основні засади забезпечення кібербезпеки України»*](https://zakon.rada.gov.ua/laws/show/2163-19#n109) *та* [*пункту 88 частини першої статті 14 Закону України «Про Державну службу спеціального зв’язку та захисту інформації України».*](https://zakon.rada.gov.ua/laws/show/3475-15#n233)

*Підвищення ефективності функціонування національної системи кібербезпеки на сьогодні є основним завданням для забезпечення сталого і безпечного функціонування національної критичної інформаційної інфраструктури в кіберпросторі, для вирішення якого впроваджується ОТМ. Її нормативне визначення - створити умови для об’єднання зусилля суб’єктів забезпечення кібербезпеки при вирішенні завдання підвищення рівня кіберстійкості критичної інформаційної 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.*

Відтак мета науково-практичного коментаря – надати практичні рекомендації органам влади щодо впровадження організаційно-технічної моделі кіберзахисту України, реалізації заходів, запропонованих [Загальними вимогами до кіберзахисту об’єктів критичної інфраструктури](https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text), [Методичними рекомендаціями щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури](https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-06-zhovtnya-2021-roku-601-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-pidvishennya-rivnya-kiberzakhistu-kritichnoyi-informaciinoyi-infrastrukturi) та іншими документами, що визначають розвиток та подальшу розбудову системи кіберзахисту національного сегмента кіберпростору.

**Науково-практичний коментар до**

**Положення  
про організаційно-технічну модель кіберзахисту, затвердженого постановою Кабінету Міністрів України від 29 грудня 2021 р. № 1426**

***Олександр Потій, Андрій Семенченко, Дмитро Дубов, Юрій Щиголь, Олександр Бакалинський, Данило Мялковський***

**Редакція 1**

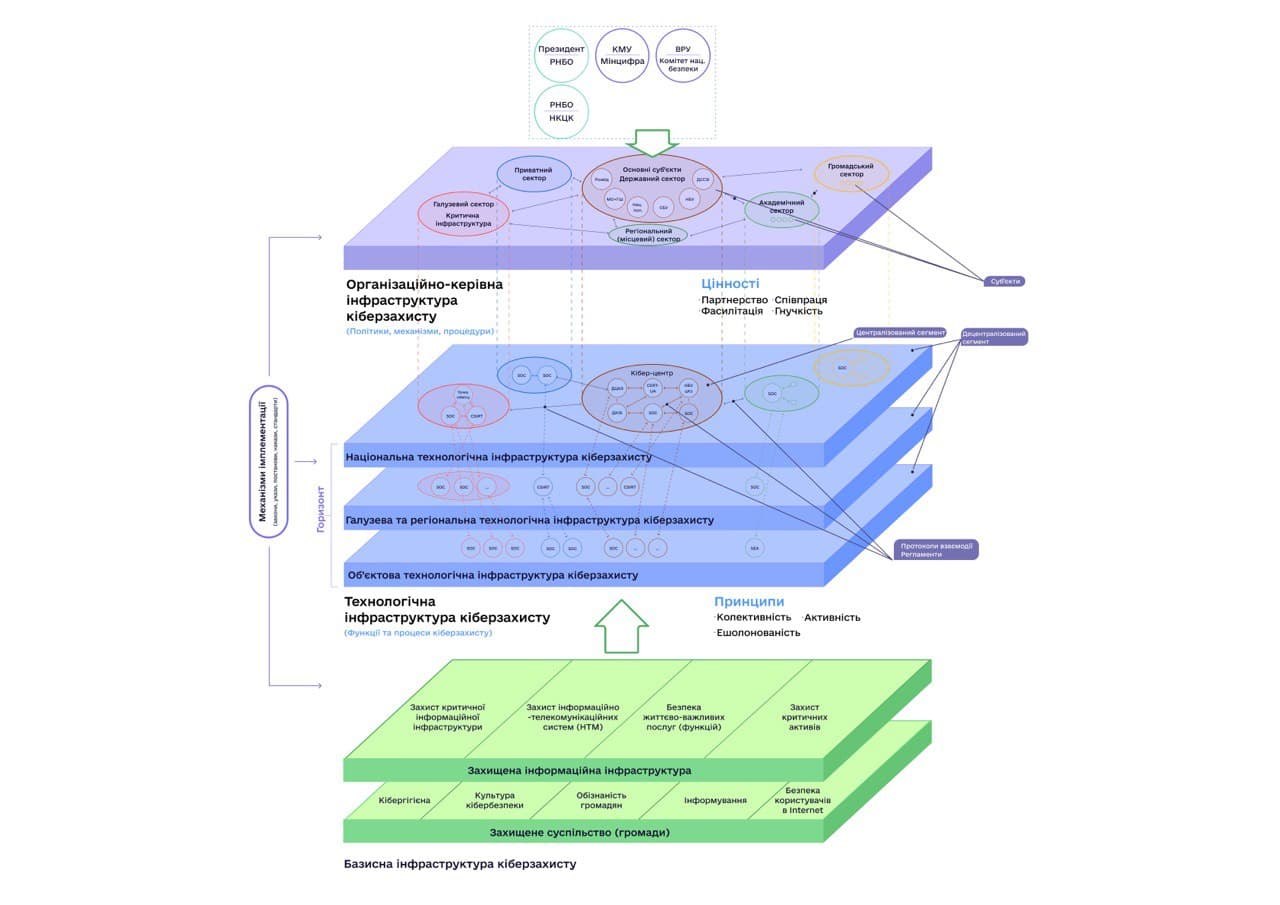
1. **Це Положення визначає механізм функціонування організаційно-технічної моделі кіберзахисту.**

**Організаційно-технічна модель кіберзахисту є комплексом заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем.**

*Виходячи з вищесказаного, можна розуміти, що організаційно-технічна модель (далі - ОТМ) кіберзахисту - така модель, яка допоможе об’єднати зусилля суб’єктів забезпечення кібербезпеки та створити умови для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, зокрема через реалізацію заходів, спрямованих на захист національних інформаційних ресурсів, кіберзахист об’єктів критичної інформаційної інфраструктури, забезпечення їх кіберстійкості, стабільного функціонування інформаційної інфраструктури державного та приватного секторів економіки.*

**Організаційно-технічна модель кіберзахисту складається з організаційно-керуючої, технологічної та базисної інфраструктури кіберзахисту та впроваджується для забезпечення функціонування національної системи кібербезпеки.**

*Такий опис ОТМ зручніше навести у вигляді певної архітектури   
(див. рис. 1), яка являє собою структуровану систему, що складається з трьох інфраструктур кіберзахисту, які взаємозалежні, взаємопов’язані і взаємодіють між собою для досягнення цілей впровадження ОТМ кіберзахисту.*

**Рис. 1 - *Архітектура ОТМ*

2. **У цьому Положенні терміни вживаються у такому значенні:**

**базисна інфраструктура кіберзахисту — організована сукупність об’єктів критичної інформаційної інфраструктури, комунікаційних і технологічних систем підприємств, установ та організацій, що належать до об’єктів критичної інфраструктури, а також суб’єктів господарювання, громадян та їх об’єднань, інших осіб, які провадять діяльність та/або надають послуги у сферах електронних комунікацій, електронної комерції, розвитку національних електронних ресурсів, захисту інформації та кібербезпеки;**

**організаційно-керуюча інфраструктура кіберзахисту — організована сукупність суб’єктів забезпечення кібербезпеки, що формують та/або реалізують державну політику у сфері кібербезпеки, визначають процедури та механізми кіберзахисту, організаційно-правові засади взаємодії між силами кіберзахисту та іншими суб’єктами забезпечення кібербезпеки;**

**технологічна інфраструктура кіберзахисту — організована сукупність сил та засобів кіберзахисту, інфраструктурних об’єктів, що забезпечують функціонування сил кіберзахисту, інформаційно-телекомунікаційних мереж та їх ресурсів, що використовуються в інтересах сил кіберзахисту;**

**сили кіберзахисту — урядова команда реагування на комп’ютерні надзвичайні події України** [**CERT-UA**](https://cert.gov.ua/)**, інші команди реагування на комп’ютерні надзвичайні події, підрозділи (групи, команди, служби) захисту інформації, підприємства, установи та організації незалежно від форми власності, які провадять діяльність та/або надають послуги, пов’язані з кіберзахистом.**

*В Україні станом на початок 2022 року існують такі команди реагування державної форми власності: урядова команда реагування на комп’ютерні надзвичайні події України* [*CERT-UA*](https://cert.gov.ua/)*, Центр кіберзахисту Національного банку України CSIRT-NBU, Ситуаційний центр забезпечення кібербезпеки СБ України, Кіберполіція, команда реагування Національного координаційного центру кібербезпеки, відповідні підрозділи ЗСУ а також підприємства, установи і організації всіх форм власності, які надають послуги кіберзахисту. Відповідно до рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави», введеного* [Указом Президента України *№ 446/2021*](https://www.president.gov.ua/documents/4462021-40009)*, здійснюється розбудова кібервійськ;*

**команди реагування на комп’ютерні надзвичайні події — групи фахівців з кібербезпеки, які утворюються з метою забезпечення кіберзахисту комунікаційних, інформаційних та/або технологічних систем.**

*Слід мати на увазі команди реагування на інциденти комп‘ютерної безпеки (CSIRT), комп’ютерні надзвичайні події (CERT), центри управління безпекою (SOC) тощо, завданням яких є обробка інцидентів комп'ютерної безпеки. Слід зазначитити, що Європейська агенція з кібербезпеки ENISA публікує рекомендації[[1]](#footnote-1) з питань створення, роботи, завдань, сервісів, налаштування та поліпшення роботи[[2]](#footnote-2), взаємодії CSIRT тощо. Окремі з них перекладені українською та опубліковані[[3]](#footnote-3) на офіційному сайті Держспецзв'язку. Нормативно загальні вимоги до CSIRT були визначені у директиві ЄС з підвищення загального рівня безпеки мереж та інформаційних систем по всьому Союзу[[4]](#footnote-4) (додаток 1) – Директиві NIS, переклад українською[[5]](#footnote-5) якої також опубліковано. На сьогодні у світі та ЄС приділяється значна увага незалежній оцінці відповідності команд реагування встановленим вимогам та публікації інформації про тих, що її підтвердили та включені у відповідні міжнародні та регіональні об’єднання таких команд. Наприклад, урядова команда CERT-UA є членом міжнародної спільноти команд реагування FIRST[[6]](#footnote-6) та об’єднання TF-CSIRT[[7]](#footnote-7). До речі, в об’єднанні TF-CSIRT перебуває також і команди реагування Національного банку України[[8]](#footnote-8) та Кредобанку[[9]](#footnote-9);*

**кібергігієна — уміння, навички користування інформаційними технологіями, спрямовані на здійснення заходів щодо своєчасного виявлення, запобігання і нейтралізації реальних і потенційних кіберзагроз.**

*Необхідно зауважити, що цей термін давно посів місце серед інших, що використовуються у сфері кібербезпеки, проте вперше отримав своє визначення у вітчизняному нормативному документі. У світі існує багато ініціатив та програм щодо впровадження кібергігієни в культуру підприємств, установ та організацій, незалежно від форми їх власності.В Україні ця сфера також отримала потужний розвиток, зокрема компанія* [*ОБСЄ*](https://www.osce.org/uk/project-coordinator-in-ukraine/505066) *з популяризації кібергігієни серед публічних службовців, CRDF Global у співпраці з експертною групою з кібербезпеки компанії EY в Україні та технічними експертами компанії Technomatix розробили онлайн-курс* [*«Базові правила безпеки у цифровому середовищі», який було проведено у чотирьох українських вишах*](https://lpnu.ua/news/bezpechnyi-onlain-abo-shcho-take-kibergigiiena)*.* [*Міністерство цифрової трансформації України та Координатор проєктів ОБСЄ*](https://www.kmu.gov.ua/news/mincifra-navchit-derzhsluzhbovciv-osnov-kibergigiyeni) *в Україні презентували освітній серіал, який розробили у співпраці з Національним агентством України з питань державної служби та Українською школою урядування в рамках проекту «Посилення спроможностей українських державних органів у сфері кібергігієни та кібербезпеки». Цей проєкт реалізовується Координатором проєктів ОБСЄ в Україні за фінансової підтримки урядів Великої Британії та Німеччини. Він рекомендується державним службовцям та посадовим особам органів місцевого самоврядування;*

**Інші терміни вживаються у значенні, наведеному в Законах України “Про основні засади забезпечення кібербезпеки України”, “Про національну безпеку України”, “Про захист інформації в інформаційно-телекомунікаційних системах”, “Про електронні довірчі послуги”.**

**3. Функціонування організаційно-технічної моделі кіберзахисту забезпечується шляхом:**

**формування та реалізації державної політики у сфері кібербезпеки, зокрема з урахуванням досвіду держав — членів ЄС та НАТО.**

*Державна політика у сфері кібербезпеки визначається сукупністю нормативно-правових актів всіх рівнів, що формують засади реалізації такої політики, її напрями, принципи та основні завдання. До ключових документів, що формують вищий (базовий) рівень такої політики, належать: Закони України «Про основні засади кібербезпеки України», «Про національну безпеку України», «Про критичну інфраструктуру», Стратегія кібербезпеки України, постанови КМУ «Про затвердження Положення про організаційно-технічну модель кіберзахисту», «Деякі питання об’єктів критичної інформаційної інфраструктури», «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом» та інші;*

**координації суб’єктів кіберзахисту під час здійснення заходів щодо забезпечення кібербезпеки об’єктів критичної інформаційної інфраструктури та національних електронних інформаційних ресурсів.**

*Під координацією суб’єктів слід розуміти, налагодження ефективного обміну інформацією про кіберінциденти, спільне реагування на інциденти, які можуть загрожувати національним інтересам, поширення найкращих практик у сфері кіберзахисту;*

**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.**

*На сьогодні українське законодавство не дає чіткого визначення «державно-приватного партнерства в сфері кібербезпеки» (ДПП). Закон України «Про основні засади кібербезпеки України» вказує на наявність «державно-приватної взаємодії» (ДПВ) і визначає шляхи, якими така взаємодія реалізується. Фактично на цей момент ДПП/ДПВ не є законодавчо визначеним певним правовим станом, а загальною рамкою, що описує заходи, які можуть вживатися суб’єктами кібербезпеки/кіберзахисту в межах наявного законодавчого поля;*

**розвитку системи кадрового, матеріально-технічного та експертно-аналітичного забезпечення сил кіберзахисту.**

*До кадрової системи забезпечення належить процес підготовки фахівців з кібербезпеки/кіберзахисту навчальними закладами всіх рівнів акредитації та будь-якої форми власності, що містить у собі їх матеріальну базу, відповідність освітніх програм потребам ринку, наявність сучасної матеріально-технічної бази, можливості підвищення кваліфікації наявних працівників суб’єктів кіберзахисту, можливість працевлаштування.*

*Система експертно-аналітичного забезпечення сил кіберзахисту - сукупність суб’єктів (організацій та окремих осіб), що проводять підготовку аналітичних матеріалів, збагачення інформації про кіберінциденти чи спроможні провести додаткову експертизу силам кіберзахисту під час попередження та виявлення кібератак, їх знешкодження та посткризового реагування, а також аналізують тенденції розвитку сфери кібербезпеки та кіберзахисту, узагальнюють найкращий світовий досвід та пропозиції щодо формування пріоритетів розвитку 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.**

*Відповідно до Закону України “Про основні засади забезпечення кібербезпеки України” Державна служба спеціального зв’язку та захисту інформації України забезпечує впровадження* [*організац*](https://zakon.rada.gov.ua/laws/show/2163-19?find=1&text=%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86+%D1%82%D0%B5%D1%85+%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C#w1_17)*ійно-*[*тех*](https://zakon.rada.gov.ua/laws/show/2163-19?find=1&text=%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86+%D1%82%D0%B5%D1%85+%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C#w2_36)*нічної* [*модел*](https://zakon.rada.gov.ua/laws/show/2163-19?find=1&text=%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86+%D1%82%D0%B5%D1%85+%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C#w3_2)*і кіберзахисту. Серед головних цілей впровадження ОТМ кіберзахисту є:*

*підвищення ефективності функціонування національної системи кібербезпеки та посилення координації дій, що здійснюються суб’єктами кіберзахисту у рамках забезпечення кібербезпеки об’єктів критичної інформаційної інфраструктури та національних інформаційних ресурсів;*

*зменшення вразливості інформаційних, комунікаційних і технологічних систем, забезпечення кіберстійкості національних інформаційних ресурсів, комунікаційних, технологічних систем та об'єктів критичної інформаційної інфраструктури;*

*створення умов для розвитку державно-приватного партнерства в інтересах кіберзахисту критичної інфраструктури;*

*створення ефективної системи національного реагування на кіберзагрози, розвиток галузевих команд реагування на кіберінциденти, синхронізація і узгодження їх дій;*

*формування сучасних спроможностей суб’єктів забезпечення кібербезпеки, зокрема сил кіберзахисту, набуття ними здатності та можливостей застосування засобів кіберзахисту відповідно до кращих світових практик, міжнародних та національних стандартів;*

*підвищення національного потенціалу в галузі безпеки у кіберпросторі, розвиток системи ресурсного забезпечення;*

*обмін інформацією щодо реалізованих та потенційних кіберзагроз та інцидентів кібербезпеки між суб’єктами забезпечення кібербезпеки, створення умов для управління кіберінцидентами, кіберкризами для стабільного соціально-економічного розвитку України;*

*забезпечення постійного контролю за станом кіберзахисту об’єктів критичної інформаційної інфраструктури та національних інформаційних ресурсів;*

*забезпечення конфіденційності, цілісності та доступності інформації та безпеки комунікаційних та технологічних систем;*

*взаємодія із системами кібербезпеки країн-членів НАТО та ЄС.*

4. **Засобами кіберзахисту, які використовуються для впровадження організаційно-технічної моделі кіберзахисту, є** [**системи виявлення вразливостей і реагування на кіберінциденти та кібератаки**](https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text)**, 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.**

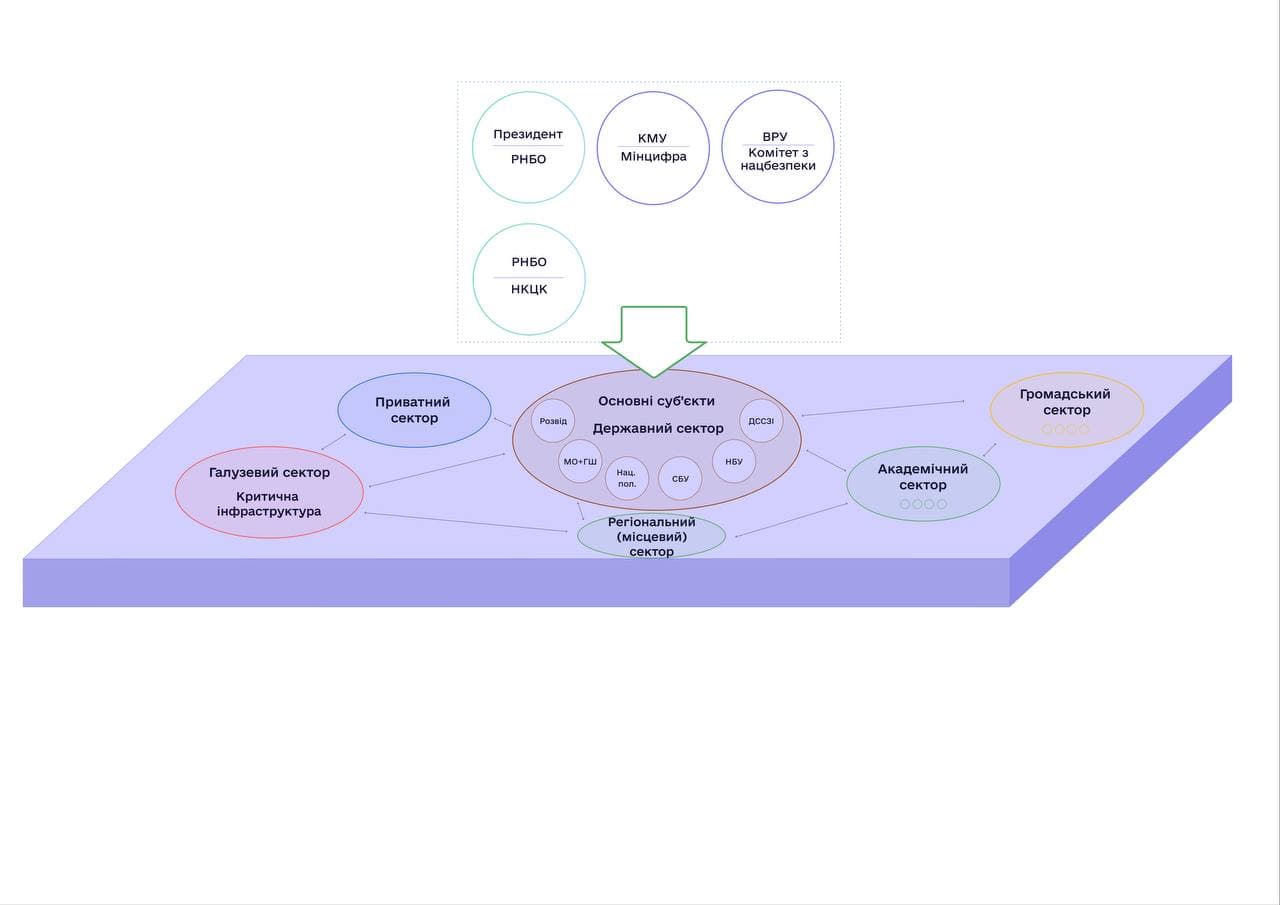
*Фактично необхідно розуміти, що мова в цьому пункті йтиметься не тільки про засоби, а й про технології кіберзахисту.*

**5. Заходами з кіберзахисту, які здійснюються у процесі впровадження організаційно-технічної моделі кіберзахисту, є організаційні, правові, інженерно-технічні заходи, 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/або співрозмірності заходів реальним та потенційним ризикам.**

*Необхідно зауважити, що має сенс як окремі складові організаційних заходів з кіберзахисту розглядати комунікативні, інформаційні, мотиваційні заходи, як заходи, спрямовані на організацію комунікації з усіма суб'єктами забезпечення кібербезпеки, на оприлюднення інформації щодо кіберінцидентів, кібератак, а також створення системи мотивації персоналу, який відповідає за забезпечення кіберзахисту критичної інфраструктури. Також як окремий напрям при впровадженні організаційно-технічної моделі необхідно визначити напрям з адаптації підходів до вирішення кібербезпекових завдань відповідно до змін безпекового середовища, визначення правил взаємодії між силами кіберзахисту та іншими заінтересованими інституціями як державної, так і приватної форми власності.*

**6. Команди реагування на комп’ютерні надзвичайні події здійснюють ідентифікацію, проводять оцінку та аналіз кіберінцидентів (кібератак), координують та беруть участь в процесі реагування на них,** [**налагоджують комунікації та інформаційний обмін щодо кіберінцидентів (кібератак)**](https://cip.gov.ua/ua/news/zagalni-pravila-obminu-informaciyeyu-pro-kiberincidenti-protokol-tlp)**, зокрема інформують інші команди реагування на комп’ютерні надзвичайні події про кіберінциденти (кібератаки), узагальнюють досвід за результатами реагування та розробляють рекомендації щодо покращення стану кіберзахисту комунікаційних, інформаційних та/або технологічних систем, здійснюють профілактичні і попереджувальні заходи щодо об’єктів кіберзахисту.**

**7. Організаційно-керуюча інфраструктура кіберзахисту складається з таких секторів (рис. 2):**

Рис. 2 - Організаційно-керуюча інфраструктура кіберзахисту

**загальнодержавний, до складу якого входять основні суб’єкти національної системи кібербезпеки,** [**сили безпеки**](https://zakon.rada.gov.ua/laws/show/2469-19#n25) **і** [**оборони**](https://zakon.rada.gov.ua/laws/show/2469-19#n26) **та Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України.**

*Основними* [*суб*](https://zakon.rada.gov.ua/laws/show/2163-19?find=1&text=%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D0%BD%D1%96+%D1%81%D1%83%D0%B1#w2_15)*’єктами національної системи кібербезпеки є 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;*

**галузевий, до складу якого входять центральні органи виконавчої влади, інші державні органи, які забезпечують формування та/або реалізацію державної політики в одній чи кількох сферах, або безпосередньо проводять відповідно до компетенції заходи із забезпечення кібербезпеки, об’єкти критичної інфраструктури незалежно від форми власності.**

*Як складові галузевого сектору необхідно розглядати уповноважені органи державної влади, відповідальні за сектор (підсектор) критичної інфраструктури. Такими на сьогодні взначені: Міненерго, Мінцифри, Мінрегіон, Мінекономіки, МОЗ, НСЗУ, НКЦПФР, Мінінфраструктури, Мінстратегпром, МВС. Вони є суб'єктами, які безпосередньо проводять відповідно до компетенції заходи із забезпечення кібербезпеки та в сфері регулювання яких є об’єкти критичної інфраструктури незалежно від форми власності. Необхідно додати, що з ухваленням Закону України “Про критичну інфраструктуру” перелік уповноважених органів суттєво розшириться. До нього можуть додатися, наприклад, Державна казначейська служба України, Міністерство захисту довкілля та природних ресурсів України, Міністерство оборони та ГШ України, СБ України, Державна судова адміністрація України, Міністерство юстиції тощо;*

**регіональний (місцевий), до складу якого входять місцеві органи виконавчої влади, органи місцевого самоврядування, підприємства, установи та організації незалежно від форми власності, що провадять діяльність у сфері захисту інформації та кіберзахисту;**

**освіти та науки (*академічний*), до складу якого входять науково-дослідні установи, заклади вищої освіти у сфері захисту інформації та кібербезпеки, що беруть участь у підготовці, підвищенні кваліфікації та перепідготовці професійних кадрів.**

*На наш погляд, до академічного сектору доцільно відносити й аналітичні центри державної, комунальної та приватної форми власності, що здійснюють освітню, наукову та експертну діяльність у сфері захисту інформації та кібербезпеки, беруть участь у підготовці, підвищенні кваліфікації та перепідготовці професійних кадрів у сфері кібербезпеки. Необхідно зауважити, що на початок 2022 року в Україні функіонує 65 закладів вищої освіти, що здійснюють освітню діяльність за спеціальністю 125 "Кібербезпека";*

**приватний, до складу якого входять підприємства недержавної форми власності, організації та установи, що провадять діяльність у сфері захисту інформації та кіберзахисту,** *інші підприємства, на яких реалізуються заходи кіберзахисту* **(крім об’єктів критичної інфраструктури);**

**громадський, до складу якого входять громадські організації, об’єднання, асоціації, спілки та фахівці у сфері кібербезпеки, а також міжнародні та міжурядові організації, що провадять свою діяльність у сфері кібербезпеки.**

*Сталою практикою у світі є введення у відповідальних за захист критичної інфраструктури органах на галузевому, регіональному рівні та на об'єктах критичної інфраструктури посади відповідальної особи за інформаційну/кібербезпеку (Chief Information Security Officer, CISO) та наділення її повноваженнями, достатніми для прийняття управлінських рішень. У таких органах необхідно сформувати окремі підрозділи з інформаційної/кібербезпеки виключно зі штатних працівників, які повинні безпосередньо підпорядковуватися CISO;*

**8. Під час функціонування організаційно-керуючої інфраструктури кіберзахисту суб’єкти забезпечення кібербезпеки:**

**здійснюють законодавче та нормативно-правове регулювання питань кіберзахисту об’єктів критичної інфраструктури, кібербезпеки та кіберзахисту комунікаційних і технологічних систем.**

*Забезпечують вироблення і адаптацію до умов, що змінюються, публічної політики у сфері кіберзахисту, створення, вдосконалення та імплементацію законодавчої бази у сфері кібербезпеки та кіберзахисту, розробку національних і галузевих стандартів та вимог у сфері кіберзахисту*;

**забезпечують гармонізацію законодавства у сфері захисту інформації, інформаційної безпеки та кібербезпеки з відповідним законодавством ЄС.**

*Забезпечують гармонізацію нормативно-правових та нормативних документів у сфері захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародного законодавства та міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО;*

**забезпечують розвиток сил кіберзахисту, системи кадрового, фінансового, матеріально-технічного та експертно-аналітичного забезпечення сил кіберзахисту.**

*Організовують заходи, спрямовані на підвищення національного потенціалу в галузі безпеки у кіберпросторі, розвиток системи ресурсного забезпечення, передусім кадрового і промислового, для потреб кібербезпеки;*

**проводять регулярні навчання щодо попередження і реагування на кіберзагрози та кіберінциденти, відновлення після кібератак;**

*До таких навчань належить командно-штабні навчання (для відпрацювання координації дій та готовності управлінської структури до кібератак) та практично-орієнтовані (перевірка навичок персоналу) навчання національного, секторального та об’єктового рівнів. Прикладами навчань національного командно-штабного рівня є: Coherent Resilience (CORE 17-21), EXECUTIVE TTX 21 тощо;*

**залучають наукові установи, професійні та громадські об’єднання до підготовки проектів законодавчих та інших нормативно-правових актів у сфері кіберзахисту.**

*Залучають експертний потенціал освітніх та наукових установ, професійних та громадських об’єднань, бізнесу до підготовки проєктів концептуальних та стратегічних документів у сфері кіберзахисту;*

**організовують і проводять** [**огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом**](https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text)**;**

**створюють умови для розвитку спроможностей сил кіберзахисту, спрямованих на виявлення кібератак та захист від них, для ліквідації їх наслідків, відновлення сталості і надійності функціонування комунікаційних та технологічних систем;**

**забезпечують впровадження сучасних принципів, методів, підходів та механізмів публічного управління в сфері кібербезпеки.**

*Розробляють та забезпечують впровадження сучасних принципів, методів, підходів, моделей та механізмів публічного управління в сфері кібербезпеки, у тому числі, тих що базуються на стратегічному плануванні та управлінні, кризовому управлінні, державно-приватній взаємодії, партнерських відносинах між державою, бізнесом та суспільством, формують звіти про ефективність регулювання у сфері кіберзахисту/кібербезпеки;*

**здійснюють співробітництво з питань кібербезпеки з органами інших держав, міжнародними, міжурядовими організаціями відповідно до компетенції та законодавства і міжнародних договорів України.**

*Розвивають стратегічні відносини з ключовими іноземними партнерами, насамперед з Європейським Союзом і НАТО та їх державами-членами, Сполученими Штатами Америки, прагматичне співробітництво з іншими державами та міжнародними організаціями на основі національних інтересів України у сфері кібербезпеки та кіберзахисту. Також це передбачає формування ефективного порядку денного під час двосторонніх та багатосторонніх кібердіалогів, визначення пріоритетів для міжнародної технічної допомоги (яка реалізується в різних формах);*

**координують дії з розроблення протоколів та регламентів взаємодії, карт технологічних процесів, регламентів робіт, планів реагування на кіберінциденти, планів відновлення та інших документів, що регламентують взаємодію між силами кіберзахисту;**

**організовують та проводять кібернавчання, розробляють програми та методики їх проведення, сценарії реагування на кіберзагрози, проводять заходи щодо протидії кіберзагрозам, з кібергігієни.**

*Головною метою діяльності суб’єктів організаційно-керуючої інфраструктури кіберзахисту є захист прав людини та національних інтересів у кіберпросторі та забезпечення глобальної та національної стабільності у кіберпросторі.*

**9. Технологічна інфраструктура кіберзахисту складається з таких рівнів:**

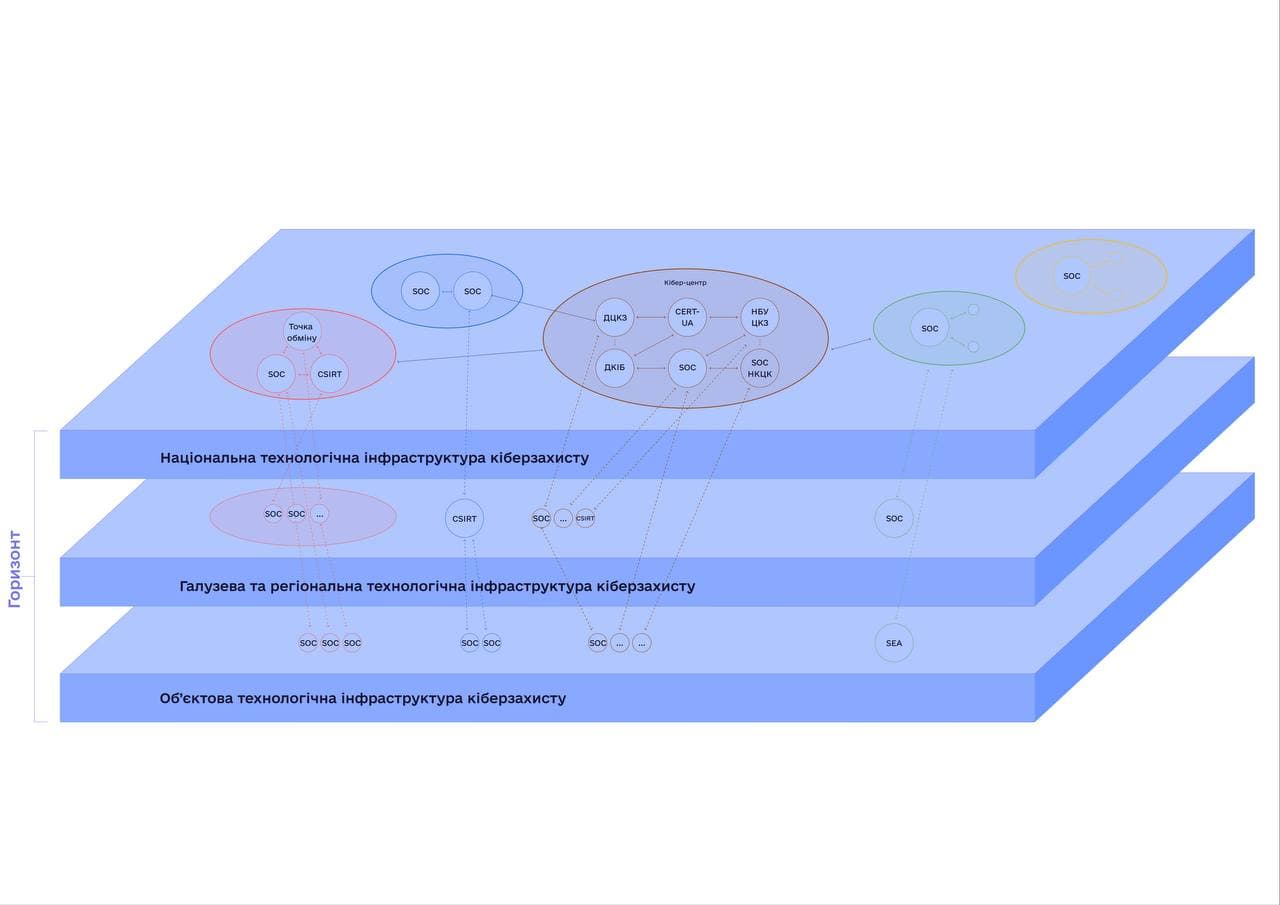


Рис. 3 - Технологічна інфраструктура кіберзахисту

**національного — на базі сил кіберзахисту основних суб’єктів національної системи кібербезпеки та Національного координаційного центру кібербезпеки як робочого органу Ради національної безпеки і оборони України.**

*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;*

**галузевого (регіонального, місцевого) — на базі сил кіберзахисту суб’єктів забезпечення кібербезпеки галузевого (регіонального) рівня;**

*Прикладами представників галузевого рівня є Операційний центр безпеки (SOC) “Укренерго”, кіберцентр "Нафтогазу", Державне підприємство «Галузевий центр цифровізації та кібербезпеки» Міністерства інфраструктури України. Триває розвиток інших галузевих підрозділів. На регіональному та місцевому рівні наявні сили кібербезпеки, представлені відповідними підрозділами Держспецзв’язку (у частині, що стосується державного контролю), СБ України та Кіберполіції;*

**об’єктового — на базі сил кіберзахисту підприємств, установ та організацій незалежно від форми власності, насамперед тих, що належать до об’єктів критичної інфраструктури.**

*Технологічна інфраструктура (див. рис. 3) формується мережею взаємодіючих технічних підрозділів кіберзахисту (CSIRTів), засобів та сервісів (служб) кіберзахисту, інформаційних систем взаємодії та обміну інформацією про кіберінциденти, кібератаки та кіберзагрози, Операційних центрів кібербезпеки (Security Operations Centers) та інших організаційно-технічних об’єктів, що забезпечують реалізацію функцій та процесів кіберзахисту в межах політик (механізмів, процедур), визначених суб’єктами кіберзахисту. Наразі Держспецзв'язку розробляє типові вимоги до Операційних центрів кібербезпеки з урахуванням вимог, розроблених* [*ENISA*](https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc)*.*

**10. Суб’єкти, що діють у технологічній інфраструктурі кіберзахисту, забезпечують оперативне (кризове) реагування на кібератаки та кіберінциденти та здійснюють обмін інформацією про ризики у сфері кібербезпеки, а також про кіберінциденти, кібератаки на:**

**національному рівні — між собою та відповідними підрозділами інших суб’єктів забезпечення кібербезпеки.**

*На національному рівні технологічна інфраструктура кіберзахисту (національна інфраструктура кіберзахисту) являє собою загальнонаціональну систему інформаційного обміну, що розгорнута на базі сил кіберзахисту основних суб’єктів національної системи кібербезпеки, які виконують функцію опорних та здійснюють обмін інформацією про кіберінциденти між собою та з відповідними підрозділами інших суб’єктів забезпечення кібербезпеки;*

**галузевому (регіональному, місцевому) рівні — з відповідними суб’єктами національного та галузевого (регіонального, місцевого) рівня технологічної інфраструктури кіберзахисту.**

*На галузевому (регіональному, місцевому) рівні (галузева (регіональна) інфраструктура кіберзахисту) технологічна інфраструктура кіберзахисту являє собою систему інформаційного обміну, що розгорнута на базі сил кіберзахисту суб’єктів забезпечення кібербезпеки галузевого (регіонального) рівня, які, не виконуючи функцію опорних, здійснюють обмін інформацією про кіберінциденти з відповідними структурами як національної, так і галузевої інфраструктури кіберзахисту;*

**об’єктовому рівні — з відповідними суб’єктами всіх рівнів технологічної інфраструктури кіберзахисту.**

*На об’єктовому рівні (об’єктова інфраструктура кіберзахисту) технологічна інфраструктура кіберзахисту являє собою систему інформаційного обміну, що розгорнута на базі сил кіберзахисту підприємств, установ та організацій будь-якої форми власності, передусім тих, які віднесені до об’єктів критичної інфраструктури, та призначена для упередження та оперативного (кризового) реагування на кібератаки та кіберінциденти, в тому числі за рахунок побудови на об’єктах критичної інфраструктури систем управління інформаційною безпекою.*

*Архітектурно кожний сегмент технологічної інфраструктури будується як оснащена засобами кіберзахисту мережа технічних підрозділів суб’єктів кіберзахисту. Така мережа складається з двох пов’язаних між собою зон – централізованої та децентралізованої.*

*Централізована зона характеризується узгодженою концентрацією (агрегацією) визначеної інформації та сервісів. Така концентрація відбувається завдяки засобам моніторингу та виявлення кіберінцидентів з метою подальшого використання для оперативного, систематичного та планового попередження суб’єктів кіберзахисту про кіберзагрози, тобто доведення інформації (поширення) до інших суб’єктів кіберзахисту. Суб’єктами централізованої зони Національної інфраструктури кіберзахисту є технічні підрозділи основних суб’єктів національної системи кібербезпеки відповідно до їх повноважень, визначених З*[*аконом України «Про основні засади забезпечення кібербезпеки України»*](https://zakon.rada.gov.ua/laws/show/2163-19#n106)*.*

*Децентралізована зона технологічної інфраструктури кіберзахисту формується усіма іншими технічними підрозділами інших секторів кіберзахисту (галузевого, регіонального, приватного, академічного громадського, місцевих органів влади), в тому числі опорних галузевих SOC ОКІ, які безпосередньо провадять у межах своєї компетенції заходи із кіберзахисту та реалізують функції кіберзахисту. Суб’єкти децентралізованої зони є постачальником визначеної інформації про події у кіберпросторі до централізованої зони через пристрої безпеки (сенсори або інші власні пристрої безпеки), тобто поширюють (розповсюджують) інформацію про аномалії, загрози тощо. Також вони є споживачами сервісів кіберзахисту, що надаються суб’єктами централізованої зони. Через власні пристрої безпеки суб’єкт децентралізованої зони виконує функції кіберзахисту власної інформаційної інфраструктури, інформаційних систем тощо, а саме: збір інформації про поточний стан функціонування пристроїв, виявлення аномалій на рівні мережевих взаємодій, моніторинг мереж та інцидентів безпеки, реагування, протидія та блокування, відновлення функціонування тощо.*

*Організаційна, технологічна та інформаційна взаємодія суб’єктів централізованої та децентралізованої зони всіх сегментів технологічної інфраструктури є ключовою умовою ефективної реалізації функцій та заходів кіберзахисту, запорукою забезпечення безпеки кіберпростору. Обмін інформацією про події у кіберпросторі є ключовим чинником попередження усіх суб'єктів кіберзахисту про кіберзагрози, а технологічна взаємодія створює умови захисту кожного суб'єкта та забезпечує функціонування системи у цілому. Масштабування технологічної інфраструктури кіберзахисту 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 можна віднести до критичної інфраструктури України. Можливість підключення до цієї платформи станом на січень 2022 року надають Держспецзв'язку, Національний координаційний центр кібербезпеки, Ситуаційний центр кібербезпеки СБ України, MISP-NBU.*

**11. Під час функціонування технологічної інфраструктури кіберзахисту сили кіберзахисту:**

**здійснюють заходи з оперативного та ефективного захисту кіберпростору щодо зменшення ризиків у сфері кібербезпеки, протидії кібератакам, кіберзлочинам, кібертероризму, кібершпигунству, а також забезпечення кібероборони та кіберрозвідки шляхом збору, аналізу, оцінювання, узагальнення та поширення інформації про ризики у сфері кібербезпеки, кіберінциденти, кібератаки;**

**здійснюють заходи з оперативного (кризового) реагування на кібератаки та кіберінциденти, зокрема за допомогою системи інформаційного обміну щодо таких подій, контрзаходи, спрямовані на усунення вразливостей комунікаційних систем;**

**здійснюють заходи з кіберзахисту об’єктів критичної інформаційної інфраструктури, комунікаційних систем, в яких обробляються національні електронні інформаційні ресурси та/або які використовуються державними органами, органами місцевого самоврядування, військовими формуваннями, утвореними відповідно до закону;**

**забезпечують функціонування систем оцінювання ризиків у сфері кібербезпеки і реагування на кіберінциденти та кібератаки щодо об’єктів кіберзахисту;**

**розвивають об’єднання (мережі) команд реагування на комп’ютерні надзвичайні події, взаємодіють з командами реагування на комп’ютерні надзвичайні події, а також підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов’язану із забезпеченням безпеки у кіберпросторі;**

**здійснюють взаємодію між собою відповідно до рішень суб’єктів забезпечення кібербезпеки;**

**інформують про кібератаки та потенційні кіберризики інших суб’єктів забезпечення кібербезпеки, опрацьовують отриману від них, зокрема від громадян, інформацію про кіберінциденти та щодо об’єктів кіберзахисту, надають консультативну та практичну допомогу з питань реагування на кібератаки;**

**сприяють державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам у вирішенні питань щодо кіберзахисту та протидії кіберзагрозам;**

**створюють та забезпечують функціонування основних складових частин системи захищеного доступу державних органів до Інтернету, системи антивірусного захисту національних електронних інформаційних ресурсів;**

**беруть участь у проведенні кібернавчань, розробленні програм та методик їх проведення, сценаріїв реагування на кіберзагрози та проводять заходи щодо протидії кіберзагрозам, з кібергігієни.**

*Головним завданням технологічної інфраструктури є оперативний та ефективний захист кіберпростору в частині протидії кібератакам, кіберзлочинам, кібертероризму, кібершпигунству, а також забезпечення кібероборони та кіберрозвідки, в т.ч. через:*

*збір, аналіз, оцінювання, узагальнення та поширення інформації про інциденти; допомогу іншим суб’єктам кіберзахисту у випадку кіберінцидентів;*

*взаємне інформування суб’єктів кіберзахисту про нові загрози;*

*створення умов для відповідального та довіреного обміну інформацією між суб’єктами кіберзахисту всіх секторів кіберзахисту.*

*Сили кіберзахисту, що діють у рамках технологічної інфраструктури:*

*провадять заходи з оперативного та ефективного захисту кіберпростору в частині протидії кібератакам, кіберзлочинам, кібертероризму, кібершпигунству, а також забезпечення кібероборони та кіберрозвідки шляхом збору, аналізу, оцінювання, узагальнення та поширення інформації про інциденти;*

*створюють системи оперативного (кризового) реагування на кібератаки та кіберінциденти (системи інформаційного обміну), впроваджують контрзаходи, спрямовані на усунення вразливостей комунікаційних систем;*

*упроваджують заходи з кіберзахисту комунікаційних систем всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, об’єктів критичної інформаційної інфраструктури, комунікаційних систем, які використовуються для задоволення суспільних потреб;*

*забезпечують функціонування систем своєчасного виявлення, запобігання та нейтралізації кіберзагроз, виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об’єктів кіберзахисту;*

*розвивають мережі команд реагування на комп’ютерні надзвичайні події, взаємодіють з українськими командами реагування на комп’ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов’язану із забезпеченням безпеки кіберпростору;*

*здійснюють взаємодію між собою на основі протоколів та регламентів взаємодії, карт технологічних процесів, регламентів робіт, планів реагування на кіберінциденти, планів відновлення та інших документів, що регламентують взаємодію;*

*інформують про наявні та потенційні загрози інших суб’єктів забезпечення кібербезпеки, опрацьовують отриману від них, у тому числі й від громадян, інформацію про кіберінциденти та кібератаки щодо об’єктів кіберзахисту, надають консультативну та практичну допомогу з питань реагування на кібератаки;*

*сприяють державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам; надають послуги із захисту інформації та кіберзахисту; створюють та забезпечують функціонування основних складових системи захищеного доступу державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів;*

*організовують та проводять кібернавчання, розробляють програми та методики їх проведення, сценарії реагування на кіберзагрози та відпрацьовують заходи протидії таким загрозам.*

**12. Здійснення заходів з кіберзахисту системами кіберзахисту передбачає:**



Рис. 4 - Цикл функцій кіберзахисту

**ідентифікацію — виявлення реальних і потенційних кіберзагроз для запобігання їм і їх нейтралізації.**

*Більш широко під ідентифікацію можна розуміти визначення користувачів і ресурсів, оцінки ризиків, оцінки вразливостей, каталогізації національних електронних інформаційні ресурсів та визначення об’єктів (активів), що підлягають кіберзахисту.* [*У*](https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-06-zhovtnya-2021-roku-601-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-pidvishennya-rivnya-kiberzakhistu-kritichnoyi-informaciinoyi-infrastrukturi)[*Методичних рекомендаціях щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури   
(далі - рекомендації) визначено, що ідентифікація*](https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-06-zhovtnya-2021-roku-601-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-pidvishennya-rivnya-kiberzakhistu-kritichnoyi-informaciinoyi-infrastrukturi) *як клас заходів з кіберзахисту передбачає заходи, реалізація яких спрямована на поглиблення знань керівництва та персоналу ОКІІ щодо наявних ризиків, способів управління ризиками кібербезпеки для інформаційних систем, активів, даних, що використовуються для надання життєво важливих послуг та функцій. Реалізація заходів кіберзахисту цього класу є чинником для ефективного використання Рекомендацій, розуміння умов, ресурсів, що підтримують надання життєво важливих послуг та функцій, а також пов'язаних ризиків кібербезпеки, обґрунтованого вибору конкретних заходів для впровадження. Це дозволяє визначити пріоритетність ризиків кібербезпеки потребами надання життєво важливих послуг та функцій, а також розподіляти ресурси і зусилля відповідно до встановлених пріоритетів;*

**захист — розроблення та впровадження методів, засобів, процедур кіберзахисту, спрямованих на забезпечення сталості і надійності функціонування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних та технологічних систем.**

*Клас заходів кіберзахисту «Кіберзахист» визначає діяльність з розробки та впровадження відповідних методів, засобів, процедур кіберзахисту для забезпечення стійкого, безперервного та безпечного надання життєво важливих послуг та функцій ОКІ. Ці заходи дозволяють обмежити або стримати вплив кіберінцидентів. До них можуть входити: контроль доступу, захист властивості даних (конфіденційність, цілісність, доступність), опис процесів та процедур, захисту від атак, технічна підтримка, тренування персоналу тощо;*

**виявлення — проведення моніторингу визначення, збору та обробки нетипових подій у кіберпросторі.**

*Фактично на етапі виявлення здійснюються збір даних про події та виявлення аномалій, моніторинг та виявлення інцидентів безпеки, побудова процесу детектування та обміну інформацією;*

**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 та/або співрозмірності можливостей таких систем реальним та потенційним ризикам;**

*Функція реагування передбачає такі кроки: підготовка до реагування, аналіз виявлених інцидентів безпеки, оцінка їх наслідків, протидія та блокування засобами захисту, інформування зацікавлених сторін щодо інцидентів, покращення системи захисту. Фактично реалізація заходів спрямована на зниження потенційного негативного впливу кіберінциденту (кібератаки) на надання життєво важливих послуг і функцій;*

**відновлення — поновлення штатного режиму функціонування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних, технологічних систем після кібератаки, відновлення інформації та відомостей у разі їх пошкодження або видалення, створення умов для проведення розслідування кібератаки.**

*Безумовно, відновлення-одна з найважливіших функцій кібербезпеки, реалізація якого починається заздалегідь із підготовки планів відновлення діяльності підприємства, елементом яких є і план відновлення після кібератаки. Не менш важливим питанням при виконанні цієї функції є завдання забезпечення проведення відповідного розслідування (як технічного - дослідження фактів та свідотств інциденту, так і за необхідності в рамках реалізації завдань оперативно-розшукової діяльності - контррозвідувального забезпечення кримінального процесу тощо), розробки та забезпечення реалізації заходів щодо вдосконалення кіберзахисту та підвищення рівня кібербезпеки.*

**13. Під час забезпечення функціонування базисної інфраструктури кіберзахисту забезпечується (рис.5):**

**захист у кіберпросторі національних електронних інформаційних ресурсів, комунікаційних і технологічних систем, зокрема тих, що використовуються для задоволення суспільних потреб;**

**захист об’єктів критичної інформаційної інфраструктури.**

*Відповідно до Закону України «Про основні засади кібербезпеки України» «об’єкт критичної інформаційної інфраструктури - комунікаційна або технологічна система об’єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об’єкта критичної інфраструктури». Положення щодо її кіберзахисту відображені в постанові КМУ від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури»;*

**захист інтересів громадянина та суспільства у кіберпросторі.**

*Зазначені інтереси прямо не визначаються чинними нормативно-правовими актами, але до них належать всі права та свободи громадянина, закріплені в Конституції України, Законах України «Про інформацію» та «Про основні засади кібербезпеки України»;*

**розроблення програм розвитку основ кібергігієни на національному, галузевому (регіональному, місцевому), об’єктовому рівні.**

**здійснення заходів з формування культури кібербезпеки в установах, на об’єктах критичної інфраструктури і підприємствах незалежно від форми власності.**

**інформування громадян про кіберінциденти.**



Рис. 5 - Базова інфраструктура кіберзахисту

*Головною метою діяльності суб’єктів на рівні базової інфраструктури є: забезпечення конфіденційності, цілісності та доступності інформації та систем, яке досягається шляхом: захисту національних інформаційних ресурсів, комунікаційних, інформаційно-комунікаційних і технологічних систем, зокрема тих, що використовуються для задоволення суспільних потреб;*

*захист критичної інформаційної інфраструктури та критичних активів; захист прав громадянина та інтересів суспільства у кіберпросторі;*

*реалізація національних та регіональних програм кібергігієни;*

*упровадження заходів формування культури кібербезпеки в установах, на об’єктах критичної інфраструктури, підприємствах всіх форм власності;*

*інформування громадян про кіберінциденти з метою підвищення їх обізнаності про небезпеку у кіберпросторі та формування практичних навичок безпечної поведінки в Інтернеті.*

**14. Базисна інфраструктура кіберзахисту функціонує для забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів у кіберпросторі.**

**

*Рис. 6 - Цикл управління ІБ*

*Розбудова базової інфраструктури кіберзахисту здійснюється шляхом впровадження* [*ризик-орієнтованого підходу*](https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#n22)[*до захисту інформації*](https://csrc.nist.gov/projects/risk-management/about-rmf)*, комунікаційних та технологічних систем, а також комплексного застосування сил та засобів захисту інформації для вирішення завдань із захисту інформаційної інфраструктури, суспільства і громадян України.*

*Забезпечення конфіденційності, цілісності та доступності інформації досягається за рахунок впровадження циклу управління інформаційною безпекою (див. рис. 6), який полягає у проведенні заходів з категоріювання безпеки, у виборі заходів захисту та їх впровадженні, проведенні оцінки безпеки, авторизації систем безпеки, моніторингу безпеки.*

**Щиголь Юрій Федорович – кандидат юридичних наук, Голова Державної служби спеціального зв’язку та захисту інформації України. Orcid ID: 0000-0002-7621-0616.**

**Потій Олександр Володимирович – доктор технічних наук, професор, заступник Голови Державної служби спеціального зв’язку та захисту інформації України. E-mail: potav1971@gmail.com. Orcid ID: 0000-0002-2366-0541.**

**Семенченко Андрій Іванович - доктор наук з державного управління, професор, директор Інституту вищих керівних кадрів Національної академії державного управління при Президентові України, лауреат Державної премії України у галузі науки і техніки, заслужений діяч науки і техніки України. E-mail: andrii.semenchenko@gmail.com. Orcid ID: 0000-0001-6482-3872.**

**Дубов Дмитро Володимирович – доктор політичних наук, старший науковий співробітник, завідувач відділу Національного інституту стратегічних досліджень. E-mail: Dmytro\_Dubov@dai.com. Orcid ID: 0000-0001-9728-369X.**

**Бакалинський Олександр Олегович – кандидат технічних наук, заступник директора Департаменту кіберзахисту Адміністрації Державної служби спеціального зв’язку та захисту інформації України. E-mail: baov@meta.ua. Orcid ID: 0000-0001-9712-2036.**

**Мялковський Данило Владиславович - кандидат наук державного управління, директор Департаменту кіберзахисту Адміністрації Державної служби спеціального зв’язку та захисту інформації України. E-mail: daniilvm71@gmail.com, Orcid ID: 0000-0002-8246-8437.**

*Це перша редакція Науково-практичного коментаря до Положення про організаційно-технічну модель кіберзахисту.*

*Коментарі та пропозиції до вищезгаданого документу просимо надавати на адресу електронної пошти* [*cyber@dsszzi.gov.ua*](mailto:cyber@dsszzi.gov.ua)*, у темі листа вказувати: «Науково-практичний коментар ОТМ». Листи без теми розглядатися не будуть.*

1. https://www.enisa.europa.eu/publications#c3=2012&c3=2022&c3=false&c5=publicationDate&reversed=on&b\_start=0&c2=CSIRT+Services. [↑](#footnote-ref-1)
2. https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc. [↑](#footnote-ref-2)
3. https://cip.gov.ua/ua/news/rekomendaciyi-enisa-yak-nalashtuvati-robotu-csirt-komanda-reaguvannya-na-incidenti-komp-yuternoyi-bezpeki-ta-soc-centr-operaciinoyi-bezpeki-kerivnictvo-z-nalezhnoyi-praktiki [↑](#footnote-ref-3)
4. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148. [↑](#footnote-ref-4)
5. https://zakon.rada.gov.ua/laws/show/984\_013-16#Text. [↑](#footnote-ref-5)
6. https://www.first.org/members/map#country%3AUA/ [↑](#footnote-ref-6)
7. https://www.trusted-introducer.org/directory/teams/cert-ua.html. [↑](#footnote-ref-7)
8. https://www.trusted-introducer.org/directory/teams/csirt-nbu-ua.html. [↑](#footnote-ref-8)
9. https://www.trusted-introducer.org/directory/teams/cert-kredobank.html. [↑](#footnote-ref-9)