Keywords: asymmetric cryptography, arithmetic operations, modular number reduction, schematic solution, algorithm, speed.

Сахибай Тинимбайович Тинимбаєв, к.т.н., професор кафедри інформаційних систем та кібербезпеки Алматинського університету енергетики та зв'язку.
E-mail:. s.tynym@gmail.com.
Orcid ID: 0000-0002-9326-9476.
Сахыбай Тынымбаевич Тынымбаев, к.т.н., профессор кафедры информационных систем и кибербезопасности Алматинского университета энергетики и связи.
Sakhybay Tynymbayev, PhD, Professor of Information Systems and Cybersecurity Academic Department, Almaty University of Power Engineering and Telecommunication.

Гнатюк Сергій Олександрович, д.т.н., доцент, заступник декана Факультету кібербезпеки, комп'ютерної та програмної інженерії Національного авіаційного університету.
E-mail: s.gnatyuk@nau.edu.ua.
Orcid ID:0000-0003-4992-0564.
Гнатюк Сергей Александрович,. д.т.н., доцент, заместитель декана Факультета кибербезопасности, компьютерной и программной инженерии Национального авиационного университета.
Sergiy Gnatyuk, DSc, Associate Professor, Vice-Dean of the Faculty of Cybersecurity, Computer and Software Engineering, National Aviation University.

Бердибаєв Рат Шиндалійович, доцент кафедри інформаційних систем та кібербезпеки Алматинського університету енергетики та зв'язку.
E-mail: r.berdybaev@aues.kz.
Orcid ID: 000-0002-8341-9645.
Бердибаев Рат Шиндалиевич, доцент кафедры информационных систем и кибербезопасности Алматинского университета энергетики и связи.
Rat Berdibayev,. PhD, Associate Professor of Information Systems and Cybersecurity Academic Department, Almaty University of Power Engineering and Telecommunication.

Поліщук Юлія Ярославівна, аспірант PhD, Національний авіаційний університет.
E-mail: liya7954@gmail.com.
Orcid ID:. 0000-0002-0686-2328.
Полищук Юлия Ярославовна, аспирант PhD, Национальный авиационный университет.
Yuliia Polishchuk, PhD student, National Aviation University.

Бурмак Юлія Анатоліївна, викладач Київського коледжу зв'язку.
E-mail: kulikovskau@gmail.com.
Orcid ID:. 0000-0002-8090-5058.
Бурмак Юлия Анатолиевна, преподаватель Киевского колледжа связи.
Yuliia Burmak, Lecturer in Kyiv College of Communication.

DOI: 10.18372/2410-7840.23.15434
УДК 004:591.5:612:616-006

КОНЦЕПТУАЛЬНІ ЗАСАДИ ВПРОВАДЖЕННЯ ОРГАНІЗАЦІЙНО-ТЕХНІЧНОЇ МОДЕЛІ КІБЕРЗАХИСТУ УКРАЇНИ

Олександр Потій, Андрій Семенченко, Дмитро Дубов, Олександр Бакалинський, Данило Мялковський

У статті запропоновано концептуальні засади впровадження організаційно – технічної моделі кіберзахисту. Зокрема, визначені її місія, мета, призначення та цілі. Вперше визначені сили та засоби кіберзахисту. Розглянуто архітектуру організаційно-технічної моделі кіберзахисту, яка являє собою структуровану систему, яка складається з трьох інфраструктур кіберзахисту, а саме: організаційно-керуючу інфраструктуру кіберзахисту, як сукупність суб'єктів забезпечення кібербезпеки, що формують та/або реалізують державну політику у сфері кібербезпеки; технологічну інфраструктуру кіберзахисту, як сукупність сил та засобів кіберзахисту, а також інфраструктури, що забезпечує функціонування сил кіберзахисту, інформаційно-комунікаційних мереж та їх ресурсів, що використовуються в інтересах сил кіберзахисту та базисну інфраструктуру кіберзахисту, як сукупність об'єктів критичної інформаційної інфраструктури, критичних активів, комунікаційних і технологічних систем підприємств, установ та організацій, що віднесені до об'єктів критичної інфраструктури, а також суб'єктів господарювання, громадян України та об'єднань громадян, інших особі, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом. Отже, впровадження організаційно-технічної моделі кіберзахисту спрямовано на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів та мінімізацію вразливості комунікаційних систем.

Ключові слова: *національна система кібербезпеки, критична інфраструктура, критична інформаційна інфраструктура, організаційно-технічна модель, кіберзахист.*

ПОСТАНОВКА ПРОБЛЕМИ

Російська агресія проти України актуалізувала значну кількість сфер національної безпеки та змусила українську державу швидко нарощувати власний безпековий потенціал. Кібербезпека стала однією з таких сфер. Хоча численні складові кібербезпеки розвивалися протягом майже всієї незалежності України, водночас до 2016 року вони не мали відповідної нормативно-правової бази, чіткої стратегії розвитку, а сама концептуальна рамка "кібербезпеки" ще в 2011-2021 роках залишалась дискусійною навіть серед суб'єктів національної системи кібербезпеки.

Російська гібридна агресія, яка в активній фазі розпочалась у 2014 році вказала на готовність агресора діяти не лише військовими та інформаційно-підривними заходами, але й у кіберпросторі проти критичної інфраструктури. Традиційно, цілі таких атак є мультиспрямованими - крім порушення штатної роботи певних об'єктів до ініціювання політичних заворушень або поширення паніки серед населення. Спроби втручання у вибори Президента України у 2014 році, кібератаки на Прикарпаттяобленерго у 2015, фінансову систему держави у 2016 та застосування кіберзброї NotPetya у 2017 - все це сформувало важливу задачу захисту національних інтересів України у кіберпросторі. При чому характер кіберскладової російської агресії вказує і на основний пріоритет діяльності російських владних хакерських груп - критична інфраструктура держави (з акцентом на енергетичний та фінансовий сектор) [1]. Така увага РФ та інших деструктивних елементів щодо діяльності в кіберпросторі пов'язана і з низкою додаткових факторів. По-перше, інформаційно-комунікаційні технології (ІКТ) все швидше стають критичними для сфери публічного управління, об'єктів критичної інфраструктури, динамічно та масштабно впроваджуються в усі сфери життєдіяльності громадян, суспільства та держави - тобто всього того, що складає простір основних заходів в межах цифрових трансформацій. Але крім позитиву це призводить також до збільшення кіберінцидентів - за деякими висновками, кількість кіберінцидентів щорічно зростає на декілька десятків відсотків, питомою частиною яких є і кіберзлочини [2-4]. По-друге, зростає ступінь вразливості суб'єктів, які здійснюють свою діяльність в Інтернеті, кіберінциденти та широкомасштабні кібератаки/операції починають наносити збитки економіці на рівні кінетичної війни, на що, зокрема, звертається увага в [4-6]. По-третє, вартість дії, які проводяться в кіберпросторі, суттєво дешевші ніж прямі військові або економічні агресивні дії. Вони також є менш ризикованими для кіберзлочинців та іноземних спеціальних служб та хакерів з позицій кримінального права та значно ефективнішими з політичної точки зору чи соціально-економічного впливу. Таким чином, загрози, які реалізуються в кіберпросторі та через кіберпростір, мають дійсно всеохопний характер та впливають на життя кожного громадянина.

Формуючи власну відповідь на вказану деструктивну кіберактивність, Україна спочатку у 2016 році ухвалила свою першу Стратегію кібербезпеки України [7], а в 2017 році - Закон України «Про основні засади забезпечення кібербезпеки України» [8]. Обидва документи підкреслюють важливість захисту критичної інфраструктури (а також "критичної інформаційної інфраструктури" як її складової), покладаючи ці обов'язки як на її власників, так і на державні органи. Також вказаний закон здійснив першу спробу визначити національну систему кібербезпеки України - її завдання, суб'єктів та виокремивши групу основних суб'єктів цієї системи, додатково вказавши їх зони відповідальності в питаннях захисту держави від кібератак.

До сьогоднішнього часу державними органами було вжито цілу низку нормативно-правових, організаційних та технічних заходів, що мали на меті імплементувати цілі та завдання зазначених стратегічних документів, і, передусім, забезпечити належний захист об'єктів критичної інфраструктури (ОКІ) держави. Це завдання ускладнювалось відсутністю чітких критеріїв визначення самого переліку ОКІ (відтак не завжди зрозуміло які об'єкти і як мають захищатись),

відсутністю критеріїв кіберзахисту для різних рівнів критичності ОКІ. Відсутнім є і базовий закон про ОКІ та їх захист, що мав унормувати значну кількість організаційно-технічних питань. Відтак «супротивник не припиняє своєї деструктивної діяльності, і кібератаки на державні органи та об'єкти критичної інфраструктури продовжуються й у 2017 р.» [8, 9].

Частково цю проблему дозволили вирішити окремі підзаконні нормативно-правові документи щодо порядку ідентифікації та категоризації критичної інфраструктури України, критичної інформаційної інфраструктури, загальних вимог з їх кіберзахисту, а також порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом [10-14].

Проте, не завжди рішення щодо зміцнення системи кібербезпеки приймались виважено та збалансовано, що пояснюється багатьма чинниками, основними з яких є те, що в систему публічного управління сферою кібербезпеки не впроваджена національна система управління ризиками кібербезпеки, завдяки якій рішення приймались би на підставі науково обгрунтованої методики. Незважаючи на вимогу закону, досі відсутні описові, організаційні, технічні, інформаційні та інші формальні моделі системи кібербезпеки (кіберзахисту), застосування яких сприяло б підвищенню ефективності та результативності управлінських та технічних рішень [15-17].

Макропроблемою є і те, що хоча юридично національна система кібербезпеки була створена, однак з моменту прийняття відповідного Закону не було запропоновано цілісну та не суперечливу організаційно-технічну модель цієї системи - більшість суб'єктів національної системи кібербезпеки залишились без визначених прав та обов'язків (крім тих, які на них покладались в межах інших законів), незрозумілим залишився характер зв'язків між ними, невизначені були форми та рівні взаємодії між різними суб'єктами. Фактично, мова йде про відсутність чітко сформульованої екосистеми кібербезпеки в якій всі її учасники тісно пов'язані між собою, доповнюють діяльність один одного, а характер відносин має здебільшого партнерський, а не адміністративно-командний характер. Закон про основні засади кібербезпеки України не ставив прямо перед державою такого завдання (створення екосистеми кібербезпеки), але вказав (так само як і Стратегія 2016 року) на необхідність розробки та впровадження організаційно-технічної моделі (ОТМ) кіберзахисту, яка частково і має вирішувати вказане завдання - визначити зміст та характер взаємодії різних суб'єктів кіберзахисту, напрямки інформаційного обміну, базові механізми запобігання, виявлення та реагування на кіберінциденти і кібератаки [18,19].

Незважаючи на те, що впровадження ОТМ як комплексу заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем» передбачено законом, її реальна розробка навіть на концептуальному рівні відсутня. До останнього часу у публічному просторі відсутні наукові та аналітичні студії, в яких би робились спроби дійсно комплексно вирішити поставлене завдання та запропонувати таку модель як для наукової дискусії, так і для її практичного впровадження, у тому числі шляхом подальшого використання у нормо-проектній роботі з питань кібербезпеки та кіберзахисту.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Організаційно-технічні аспекти розбудови систем кібербезпеки різних країн розглядались в їх національних стратегіях кібербезпеки, рекомендаціях ENISA, ITU, NATO [20-23], працях зарубіжних та вітчизняних вчених:, Дж. Ліпмана, А. Льюїса, Д. Крамера, Р. Олдрича, В. Шарпа, М. Шмітта, Б. Шнаєра, Keir Giles, Kim Hartmann, Robert S. Dewar, В. Бурячка, Р. Грищука, О. Довганя, Д. Дубова, А.Семенченко, В.Мохора, О.Корченка, В.Цуркана та ін.

Однак, незважаючи на значну кількість робіт, варто зазначити, що в Україні недостатньо досліджень саме з питань розбудови організацій-

но-технічної моделі кіберзахисту та з розвитку національної системи кібербезпеки в цілому.

Відтак **мета статті** – розробити концептуальні засади формування та впровадження організаційно-технічної моделі кіберзахисту України та обґрунтувати практичні рекомендації органам влади щодо їх впровадження.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Відповідно до [8] одним з шляхів забезпечення функціонування національної системи кібербезпеки є впровадження організаційно-технічної моделі (далі - ОТМ) національної системи кібербезпеки як комплексу заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем.

Місія ОТМ кіберзахисту – через розвиток зрілості (maturity) національної системи кібербезпеки забезпечити її стійкість (resilience) задля безпечного та сталого функціонування українських об'єктів критичної інфраструктури, систем надання електронних послуг, інформаційної інфраструктури, нейтралізації (зменшення наслідків) кібератак та кіберінцидентів. Метою впровадження ОТМ кіберзахисту є досягнення Україною високого рівня координації та реалізації ініціатив щодо побудови національної системи кібербезпеки, захисту національних інформаційних ресурсів, стабільного функціонування інформаційної інфраструктури державних установ, галузей економіки та бізнесу, отримання соціально-економічних зисків від надійного та безпечного функціонування кіберпростору, що відповідає міжнародним зобов'язанням України та вимогам [8, 20].

Зважаючи на своє призначення, ОТМ кіберзахисту має створити умови та об'єднати зусилля суб'єктів забезпечення кібербезпеки 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.

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 та 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 інциденти 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 з системами кібербезпеки країн НАТО та ЄС.

Силами кіберзахисту, які залучаються до впровадження ОТМ кіберзахисту, є урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, галузеві команди реагування на комп'ютерні надзвичайні події, підрозділи (групи, команди, служби) та/або фахівці суб'єктів забезпечення кібербезпеки, які безпосередньо здійснюють у межах своєї компетенції заходи з кіберзахисту та захисту інформації та/або надають послуги, у цих сферах.

Технологіями та засобами кіберзахисту, які використовуються для реалізації ОТМ кіберзахисту, є системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, інформаційні технології, технічні, програмні та програмно-апаратні засоби (пристрої, обладнання, комплекси), які використовуються в інтересах забезпечення кіберзахисту державних інформаційних ресурсів, комунікаційних та технологічних систем, а також об'єктів критичної інформаційної інфраструктури.

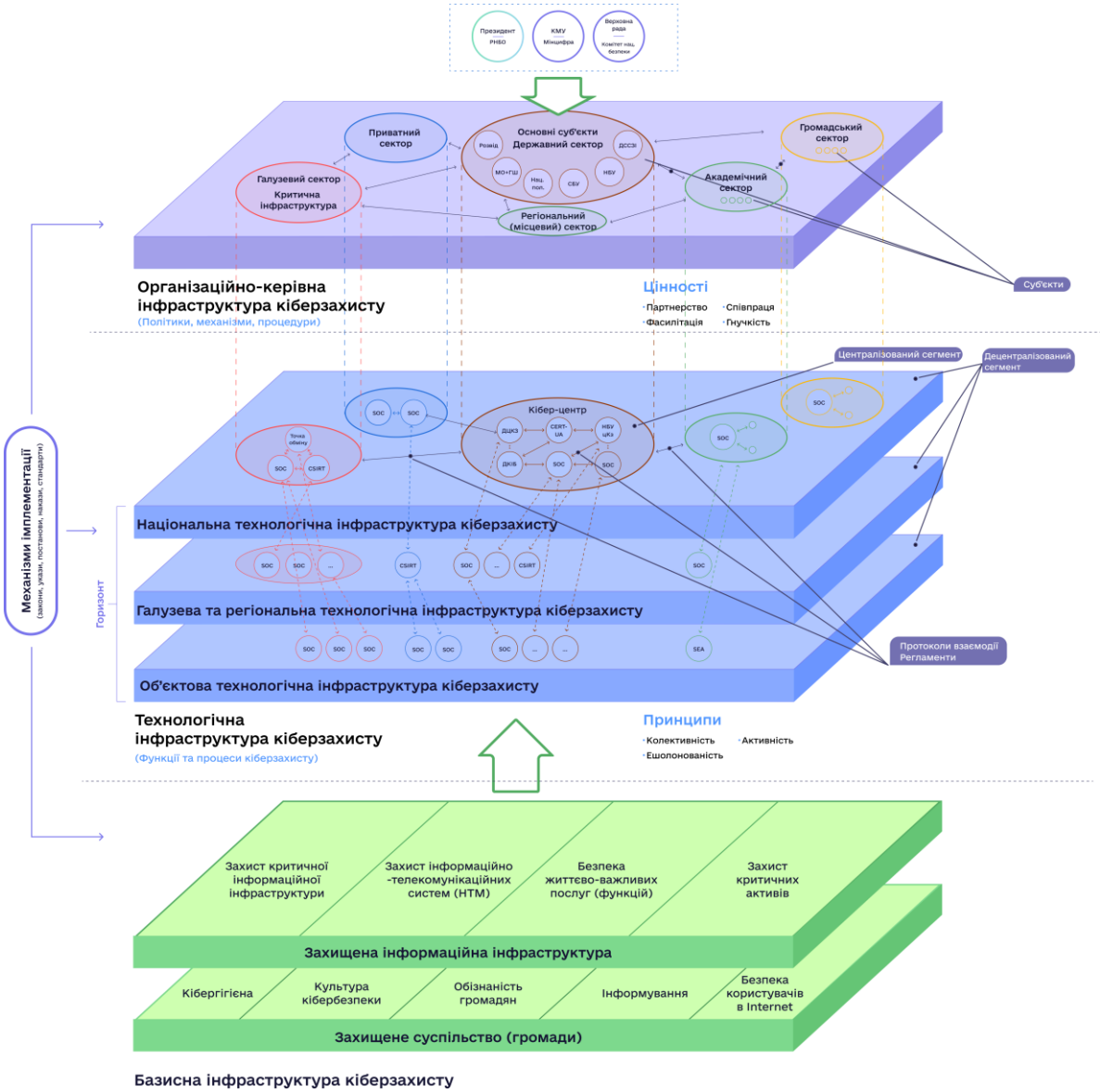

Рис.1 Архітектура організаційно-технічної моделі

Заходами з кіберзахисту, які реалізуються у процесі впровадження ОТМ кіберзахисту, є організаційні, правові, комунікативні, інформаційні, мотиваційні, інженерно-технічні заходи, заходи криптографічного та технічного захисту інформації, які здійснюються силами кіберзахисту та

базуються на принципах персональної відповідальності за власні дії та колективної відповідальності за безпеку кожного, адаптації підходів до вирішення кібербезпекових завдань відповідно до змін безпекового середовища; правила взаємодії між силами кіберзахисту та іншими заінтересованими інституціями як державної, так і приватної форми власності.

Архітектура ОТМ (див. рис.1) кіберзахисту являє собою структуровану систему, яка складається з трьох інфраструктур кіберзахисту, що взаємозалежні, взаємопов'язані і взаємодіють між собою для досягнення цілей впровадження ОТМ кіберзахисту, а саме:

– організаційно-керуюча інфраструктура кіберзахисту, як сукупність суб'єктів забезпечення кібербезпеки, що формують та/або реалізують державну політику у сфері кібербезпеки, визначають процедури та механізми кіберзахисту, встановлюють організаційно-правові засади взаємодії між силами кіберзахисту та іншими заінтересованими інституціями як державної, так і приватної форми власності;

– технологічна інфраструктура кіберзахисту, як сукупність сил, технологій та засобів кіберзахисту, а також інфраструктури, що забезпечує функціонування сил кіберзахисту, інформаційно-комунікаційних мереж та їх ресурсів, що використовуються в інтересах сил кіберзахисту;

– базисна інфраструктура кіберзахисту, як сукупність об'єктів критичної інформаційної інфраструктури, критичних активів, комунікаційних і технологічних систем підприємств, установ та організацій, що віднесені до об'єктів критичної інфраструктури, а також суб'єктів господарювання, громадян України та об'єднань громадян, інших особі, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

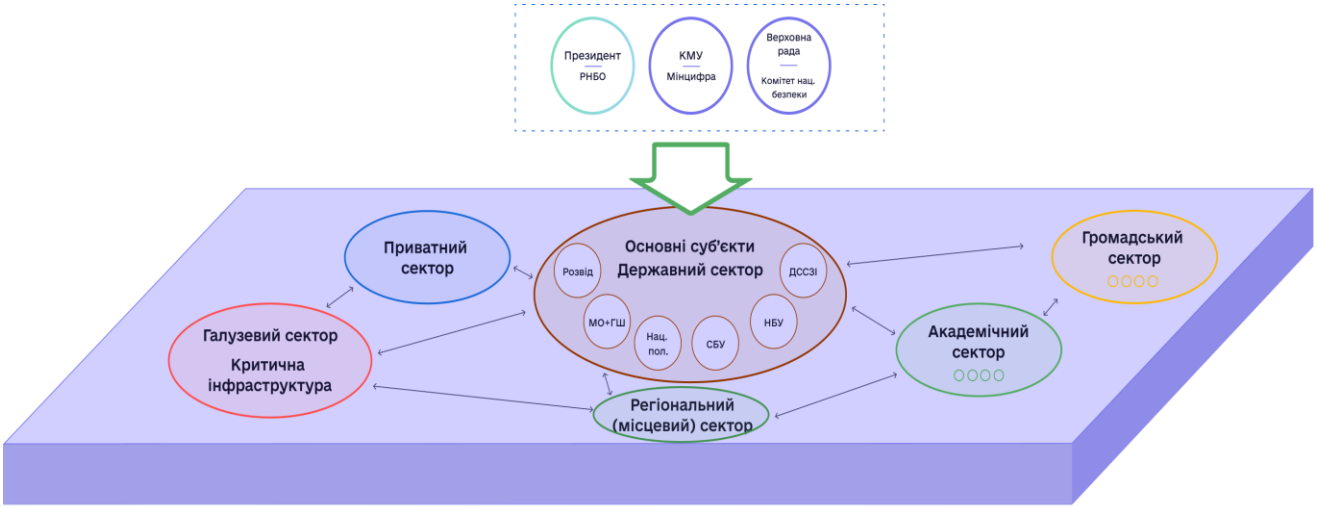

Рис. 2 Організаційно-керуюча інфраструктура кіберзахисту

Організаційно-керуюча інфраструктура кіберзахисту (див. рис.2) ґрунтується на функціонуванні та взаємодії п'яти стратегічних груп стейкхолдерів (з підмножинами їхніх суб'єктів), що формують відповідні сектори кіберзахисту:

–загальнодержавний, до складу якого входять Президент України, вищі органи державної влади;

–галузевий, до складу якого входять державні органи, які забезпечують формування та/або реалізацію державної політики в одній чи кількох сферах, об'єкти критичної інфраструктури всіх форм власності;

–регіональний (місцевий), до складу якого входять місцеві органи виконавчої влади та органи місцевого самоврядування, комунальні підприємства, організації, установи, що здійснюють діяльність в сфері захисту інформації та кібербезпеки;

–приватний, до складу якого входять підприємства недержавної форми власності, організації та установи, що здійснюють діяльність в

сфері захисту інформації та кібербезпеки, інші підприємства, на яких реалізуються заходи кіберзахисту (крім об'єктів критичної інфраструктури);

–академічний, до складу якого входять науково-дослідні установи, заклади вищої освіти, аналітичні центри державної, комунальної та приватної форми власності, що здійснюють освітню, наукову та експертну діяльність в сфері захисту інформації та кібербезпеки, беруть участь у підготовці, підвищенні кваліфікації та перепідготовці професійних кадрів в сфері кібербезпеки;

–громадський, до складу якого входять громадські організації, об'єднання, асоціації, спілки та представники експертного середовища в сфері кібербезпеки, а також міжнародні партнери України, що здійснюють свою діяльність у сфері кібербезпеки.

Суб'єкти забезпечення кібербезпеки, що діють на рівні організаційно-керуючої інфраструктури кіберзахисту:

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

– 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;

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

– залучають експертний потенціал освітніх та наукових установ, професійних та громадських об'єднань, бізнесу до підготовки проектів концептуальних та стратегічних документів у сфері кіберзахисту;

– організовують та проводять огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом;

– створюють умови для розвитку спроможностей сил кіберзахисту, спрямованих на упередження, запобігання, виявлення та захисту від кібератак, ліквідації їх наслідків, відновлення сталості і надійності функціонування, комунікаційних та технологічних систем;

– 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, кризисному управлінні, державно-приватній взаємодії, партнерських відносинах між державою, бізнесом та суспільством, формують звіти про ефективність регулювання в сфері кіберзахисту/кібербезпеки;

– 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.

Головною метою діяльності суб'єктів організаційно-курую ті інфраструктури кіберзахисту є захист прав людини та національних інтересів у кіберпросторі та забезпечення глобальної та національної стабільності у кіберпросторі. 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.

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.

Реалізація цього завдання ґрунтується на впровадженні на всіх рівнях циклу функцій кіберзахисту (див. рис. 4), який включає в себе:

– ідентифікацію – визначення користувачів та ресурсів, оцінки ризиків, оцінки вразливостей, каталогізації національних електронних інформаційні ресурсів та визначення об'єктів (активів), що підлягають кіберзахисту

– захист – контроль доступу, захисту даних (конфіденційність, цілісність, доступність), опис процесів та процедур, захисту від атак, технічної підтримки, тренування персоналу;

– виявлення – збір подій та виявлення аномалій, моніторинг та виявлення інцидентів безпеки, побудова процесу детектування та обміну інформацією;

– реагування – аналіз інцидентів безпеки, оцінки їх наслідків, протидії та блокуванню засобами захисту, покращення системи захисту;

– відновлення – відновлення після кібератаки, забезпечення проведення відповідного їх розслідування, розробки та забезпечення реалізації заходів щодо вдосконалення системи кіберзахисту та підвищенння рівня кібербезпеки.

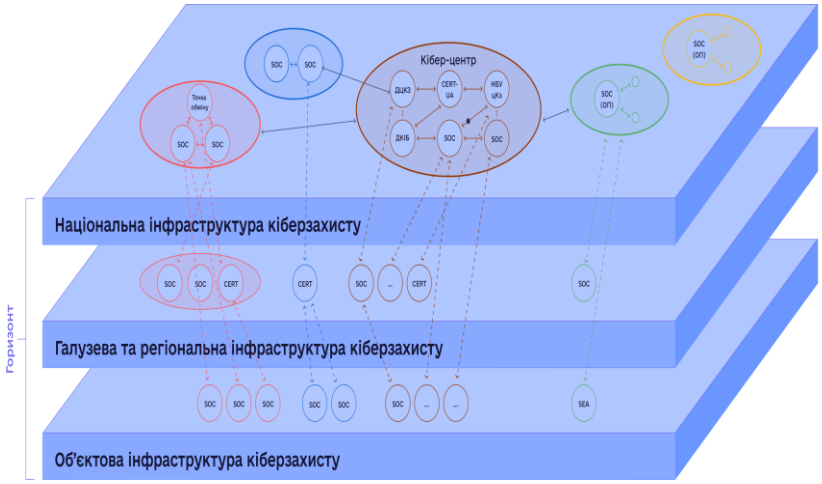

Рис. 3 Технологічна інфраструктура кіберзахисту

Рис. 4 Цикл функцій кіберзахисту

Технологічна інфраструктура кіберзахисту розбудовується на національному, галузевому (регіональному, місцевому) та об'єктовому рівнях.

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.

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.

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 [12, 24, 25].

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 поширення інформації (доведення) 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 Законом України «Про основні засади забезпечення кібербезпеки України»

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 здійснюють 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.

Сили кіберзахисту, що діють у рамках технологічної інфраструктури:

–здійснюють 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;

–впроваджують 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.

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 [26].

Обмін інформацією про події у кіберпросторі є ключовим чинником попередження усіх суб'єктів кіберзахисту про кіберзагрози, а технологічна взаємодія створює умови захисту кожного суб'єкту та забезпечує функціонування системи у цілому.

Масштабування технологічної інфраструктури кіберзахисту здійснюється за рахунок поступового збільшення (у відповідності 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.

Базова інфраструктура кіберзахисту (див. рис.5) складається з двох шарів , які взаємопов'язані ціллю захисту конфіденційності, цілісності та доступності інформації, а саме:

–захищена інформаційна інфраструктура України;

–захищені суспільство і громадяни України.

Головною метою діяльності суб'єктів на рівні базової інфраструктури є забезпечення конфіденційності, цілостності та доступності інформації та систем.

Це досягається здійснюється шляхом [27]:

–захисту національних інформаційних ресурсів, комунікаційних, інформаційно-комунікаційних і технологічних систем, зокрема тих, що використовуються для задоволення суспільних потреб;

–захисту критичної інформаційної інфраструктури та критичних активів;

–захисту прав громадянина та інтересів суспільства у кіберпросторі;

–реалізації національних та регіональних програм кібергігієни;

–впровадження 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.

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

Розбудова базової інфраструктури кіберзахисту здійснюється шляхом впровадження ризик-орієнтований підходу до захисту інформації, комунікаційних та технологічних систем, а також комплексного застосування сил та засобівзахисту інформації до вирішення завдань із захисту інформаційної інфраструктури, суспільства і громадян України. На рис. 7 представлена загальна концепція організаційно-технічної моделі кіберзахисту

Рис. 5 Базова інфраструктура кіберзахисту

Рис. 6 Цикл управління ІБ

Рис. 7 Організаційно-технічна модель кіберзахисту

ВИСНОВКИ

Проаналізовано стан розробки та впровадження в Україні ОТМ кіберзахисту, доведено актуальність створення. Вперше запропоновано концептуальні засади формування та впровадження організаційно-технічної моделі кіберзахисту України що включають визначення місії, мети, головних цілей ОТМ, сил, засобів, заходів кіберзахисту, архітектури ОТМ кіберзахисту. Розкрито сутність, склад та завдання кожної з складових архітектури ОТМ кіберзахисту на національному, галузевому (регіональному, місцевому) та об'єктовому рівнях: організаційно-керуючої, технологічної та базисної інфраструктури кіберзахисту. Обґрунтовано як базовий централізовано-децентралізований принцип розбудови ОТМ кіберзахисту. Нормативно-правове закріплення ОТМ кіберзахисту дасть можливість здійснювати її розвиток планово, на підставі збалансованих ьа обгрунтованих 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.

ЛІТЕРАТУРА

[1] Андрей Бродецкий *Три года NotPetya. Как это было и готова ли Украина к новым атакам?* режим доступу -https://project.liga.net/projects/ notpetya_3years/.

[2] Організаційно-правові механізми розвитку національної системи кібербезпеки України: стан та перспективи І. Б. Жиляєв, А. І. Семенченко // *Стратегічні пріоритети*. - 2017. - № 4. - С. 55-63. - режим доступу: http://nbuv.gov.ua/UJRN/spa_2017_4_8.

[3] Дубов Д. В. *Кіберпростір як новий вимір геополітичного суперництва: монографія* / Д. В. Дубов. – К.: НІСД, 2014. – 328 с.

[4] *EU Cybersecurity Act*, - режим доступу: https://ec.europa.eu/digital-single-market/en/eu-cyber security-act.

[5] *Проєкт Стратегії кібербезпеки України (2021 – 2025 роки)* - режим доступу: https://www.rnbo. gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf.

[6] Дубов Д. В. *Формуючи нову стратегію кібербезпеки України: чи можемо уникнути помилок першої спроби стратегування?* / Д. В. Дубов – К. : НІСД, 2021. – 6 с., - режим доступу: https:// niss.gov.ua /sites /default/files/2021-01/tezy-dubov-2.pdf.

[7] *Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року* режим доступу: https://zakon.rada.gov.ua/laws/show/96/2016#Text.

[8] *Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2017 році»*. – К.: НІСД, 2017. – 928 с.

[9] *Cybesecurity in Ukraine: problems and perspectives* O.Potii, O.Korneyko, Y.Gorbenko - Information and Secu rity: An International Journal, vol.32 (2015), 2015. – pp. 3201-1-24.

[10] *Деякі питання об'єктів критичної інфраструктури, Постанова Кабінету Міністрів України № 1109 від 9 жовтня 2020 р.* - режим доступу: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.

[11] *Деякі питання об'єктів критичної інформаційної інфраструктури, Постанова Кабінету Міністрів України № 943 від 9 жовтня 2020 р.* - режим доступу: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text.

[12] *Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, Постанова Кабінету Міністрів України № 518 від 19 червня 2019 року.Офіційний вісник України від 02.07.2019. 2019,* № 50, стор. 53, стаття 1697, код акту 94896/2019.

[13] *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 № 1176 від 11 листопада 2020 р.* - режим доступу: https://zakon.rada.gov.ua /laws/ show/1176-2020-%D0%BF#Text.

[14] *Правове забезпечення кібербезпеки в Україні* О.Бакалінська, О.Бакалинський - Підприємництво, господарство і право, 2019. http://pgp-journal.kiev.ua/archive/2019/9/18.pdf.

[15] *ДСТУ ISO/IEC 15408-1:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель* (ISO/IEC 15408-1:2009, IDT).

[16] Дубов Д.В. *Кіберпростір як новий вимір геополітичного суперництва: монографія* / Д.В. Дубов.- К.: НІСД, 2014. - 328 с.

[17] Гончар С.Ф. *Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури: монографія.* Київ : Альфа реклама, 2019. 176 с.

[18] Potii O. Advanced security assurance case based on ISO/IEC 15408 / O. Potii, O. Illiashenko, D. Komin // *Theory and Engineering of Complex Systems and Dependability*, 2015. – pp. 391-401.

[19] *Українські вчені розробили концепцію організаційно-технічної моделі кіберзахисту* - режим доступу: https://www.unn.com.ua/uk/news/1903577-ukra

yinski-vcheni-rozrobili-kontseptsiyu-organizatsiyno-tekhnichnoyi-modeli-kiberzakhistu.

[20] *National Cyber Security Strategy 2016-2021*, - режим доступу: https://www.itu.int/en/ITU-D/ Cyber security/Documents/National_Strategies_Repository /national_cyber_security_strategy.pdf.

[21] National Cyber Security Framework Manual, - режим доступу: https://www.ccdcoe.org/uploads/2018/10 /NCSFM_0.pdf.

[22] *National Cybersecurity Strategies*, - режим доступу: https://www.enisa.europa.eu/topics/national-cyber-security-strategies.

[23] *Директива Європейського Парламенту і Ради (ЄС) «Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» від 6 липня 2016 року 2016/1148* - режим доступу: https://zakon.rada.gov.ua/laws/show/984_013-16# Text.

[24] О.Бакалинський *Модель та методи визначення проектних характеристик систем управління інформаційною безпекою: монографія.* Київ : ТОВ «Три К», 2020. – 162 с.

[25] Метод концептуалізування системних досліджень систем управління інформаційною безпекою, В.Мохор, В.Цуркан, О.Бакалинський, Я.Дорогий – *Збірник "Information Technology and Security"*, 2020 - режим доступу: http://its.iszzi.kpi.ua/article/view/218012.

[26] Мялковський Д.В. Стратегічне управління розвитком кіберзахисту критичної інформаційної інфраструктури України / І.Б. Жиляєв, А.І. Семенченко, Д.В. Мялковський, Т.В. Станіславський. *Публічне управління та адміністрування в Україні*. Одеса, 2018. №3. С. 44-51 (в частині пропозицій до визначення об'єктів критичної інфраструктури у сфері телекомунікацій та цифрових послуг).

[27] Семенченко А.І., Мялковскій Д.В. Розвиток інституційних спроможностей суб'єктів забезпечення системи кібербезпеки та кіберзахисту України /А.І.Семенченко, Д.В.Мялковскій/Теорія та практика державного управління Вид-во ХарРІ НАДУ "Магістр", 2020.-Вип. 3(70).-С.40-54.

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ВНЕДРЕНИЯ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ МОДЕЛИ КИБЕРЗАЩИТЫ УКРАИНЫ

В статье предложены концептуальные основы внедрения организационно - технической модели киберзащиты. В частности, определены ее миссия, цель, назначение и главные цели. Впервые определены силы и средства киберзащиты. Рассмотрено архитектуру организационно-технической модели киберзащиты, которая представляет собой структурированную систему, состоящую из трех инфраструктур киберзащиты, а именно: организационно-управляющей инфраструктуры киберзащиты, как совокупности субъектов обеспечения кибербезопасности, формирующих и/или реализующих государственную политику в сфере кибербезопасности; технологической инфраструктуры киберзащиты, как совокупности сил и средств киберзащиты, а также инфраструктуры, обеспечивающей функционирование сил киберзащиты, информационно-коммуникационных сетей и их ресурсов, используемых в интересах сил киберзащиты и базовой инфраструктуры киберзащиты, как совокупности объектов критической информационной инфраструктуры, критических активов, коммуникационных и технологических систем предприятий, учреждений и организаций, отнесенных к объектам критической инфраструктуры, а также субъектов хозяйствования, граждан Украины и объединений граждан, других лице, осуществляющих деятельность и/или предоставляют услуги, связанные с национальными информационными ресурсами, информационными электронными услугами, осуществлением электронных сделок, электронными коммуникациями, защитой информации и киберзащиты. Таким образом, внедрение организационно-технической модели киберзащиты направлено на оперативное (кризисное) реагирования на кибератаки и киберинциденты, внедрения контрмер и минимизации уязвимости коммуникационных систем.

Ключевые слова: национальная система кибербезопасности, критическая инфраструктура, критическая информационная инфраструктура, организационно-техническая модель, киберзащита.

CONCEPTUAL PRINCIPLES OF IMPLEMENTATION OF THE ORGANIZATIONAL AND TECHNICAL MODEL OF CYBER DEFENSE OF UKRAINE

The conceptual bases of introduction of organizational - technical model of cybersecurity are offered in the article. In particular, its mission, purpose, purpose and goals are defined. For the first time, the forces and means of cyber defense have been identified. The architecture of organizational and technical model of cybersecurity is considered, which is a structured system consisting of three cybersecurity infrastructures, namely: organizational and management infrastructure of cybersecurity, as a set of cybersecurity entities that form and / or implement state policy in the field of cybersecurity; cyber security technological infrastructure, as a set of cyber security forces and means, as well as infrastructure that ensures the functioning of cyber security forces, information and communication networks and their resources used in the interests of cyber defense forces and basic cyber security infrastructure, as a set of critical information infrastructure, critical assets, communication and technological systems of enterprises, institutions and organizations related to critical infrastructure, as well as business entities, citizens of Ukraine and associations of citizens, other persons who

carry out activities and / or provide services, related to national information resources, electronic information services, electronic transactions, electronic communications, information protection and cyber security. Thus, the implementation of the organizational and technical model of cyber defense is aimed at rapid (crisis) response to cyber attacks and cyber incidents, the introduction of countermeasures and minimizing the vulnerability of communication systems.
Keywords: national cybersecurity system, critical infrastructure, critical information infrastructure, organizational and technical model, cybersecurity.

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.
Потий Александр Владимирович - доктор технических наук, профессор, заместитель Председателя Государственной службы специальной связи и защиты информации Украины.
Oleksandr Potii - Doctor of Technical Sciences, Professor, Deputy Head of the State Service for Special Communications and Information Protection of Ukraine.

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.
Семенченко Андрей Иванович - доктор наук государственного управления, профессор, директор Института высших руководящих кадров Национальной академии государственного управления при Президенте Украины, лауреат Государственной премии Украины в области науки и техники, заслуженный деятель науки и техники Украины.
Semenchenko Andriy - Doctor of Science in Public Administration, Professor, Director of the Institute of Senior Management of the National Academy of Public Administration under the President of Ukraine, laureate of the State Prize of Ukraine in Science and Technology, Honored Worker of Science and Technology of Ukraine.

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.
Дубов Дмитрий Владимирович - доктор политических наук, старший научный сотрудник, заведующий отделом Национального института стратегических исследований.
Dubov Dmytro - Doctor of Political Sciences, Senior Researcher, Head of the Department of the National Institute for Strategic Studies.

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.
Бакалинський Александр Олегович - кандидат технических наук, заместитель директора Департамента киберзащиты Администрации Государственной службы специальной связи и защиты информации Украины.
Bakalynsky Oleksandr - Candidate of Technical Sciences, Deputy Director of the Department of Cyber Defense of the Administration of the State Service for Special Communications and Information Protection of Ukraine.

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.
Мялковський Даниил Владиславович - кандидат наук государственного управления, директор Департамента киберзащиты Администрации Государственной службы специальной связи и защиты информации Украины,
Myalkovsky Danylo - Candidate of Sciences of Public Administration, Director of the Department of Cyber Defense of the Administration of the State Service for Special Communications and Information Protection of Ukraine.