Аналітична записка
з питань порівняльного законодавства
щодо правових засад забезпечення та організації системи кібербезпеки та захисту державних інформаційних ресурсів у ЄС, державах-членах ЄС, а також в США, Ізраїлі, Південній Кореї*

Анотація. *Викладено результати аналізу правових засад, способів організації та механізмів регулювання систем кібербезпеки та захисту державних інформаційних ресурсів у ЄС, окремих державах-членах ЄС, а також США, Ізраїлі та Південній Кореї. Проаналізовано стратегічні документи і законодавчі акти, що визначають пріоритети та напрями політики ЄС, окремих держав у питанні організації систем національної безпеки, а також взаємоузгоджених заходів кіберзахисту, що здійснюються ними.*

Ключові слова: *державні інформаційні ресурси, кіберінцидент, кібербезпека, кіберзахист, кіберзагроза, кіберзлочин, кіберпростір, національна безпека, національний координатор у сфері кібербезпеки, національна система кібербезпеки.*

Вступ. Безпека в кіберпросторі та кіберзахист національних інформаційних ресурсів є ключовою складовою національної безпеки та оборони кожної держави. Актуальність цих питань щороку зростає і пов'язана не лише з посиленням технічних можливостей кіберзлочинності, а й з глобальними загрозами. Кожна держава у протидії цьому і задля захисту національних інтересів, збереження суверенності створює національні системи кібербезпеки як формат співробітництва державних органів, установ, організацій, приватного сектору, наукових установ і організацій, професійних асоціацій та неурядових організацій у цій сфері.

Положеннями Стратегії кібербезпеки[1] і Закону України «Про основні засади забезпечення кібербезпеки України»[2] сформовано розуміння національної системи кіберзахисту України та її структуру. Відповідно до частин першої-четвертої статті 5, частин першої та другої статті 8 цього Закону визначено широке коло суб'єктів забезпечення кібербезпеки – від Президента, (діє через Національний координаційний центр кібербезпеки) до громадян України, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами тощо. Крім того, Законом визначено термін «національна система кібербезпеки», а також перелік функціональних органів державної влади, які безпосередньо залучаються до виконання завдань щодо її забезпечення.

---

[1] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text
Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України : Розпорядження Кабінету Міністрів України від 19 грудня 2023 року № 1163. URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennia-planu-zakhodiv-na-20232024-roky-z-realizatsii-stratehii-kiberbezpeky-ukrainy-i191223-1163

[2] Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

Врахування іноземного досвіду організації систем кіберзахисту є надзвичайно актуальним для України. Адже питання кібербезпеки виходить за межі суто національного регулювання, оскільки стосується забезпечення глобального захисту в кіберпросторі та вимагає узгоджених дій її суб'єктів у всьому світі. Зокрема, 21 грудня 2024 року уряд затвердив зміни до «Положення про організаційно-технічну модель кіберзахисту»[3], якими передбачається впровадження єдиного підходу до забезпечення кіберзахисту інформаційно-комунікаційних систем державних органів та об'єктів критичної інфраструктури, що ґрунтується на положеннях Cybersecurity Framework 2.0 від Національного інституту стандартів та технологій США (далі – NIST)[4].

Основна частина. Правовим відліком *(Додаток 1)* поточного етапу розвитку політики кібербезпеки ***ЄС*** стало прийняття у 2020 році Стратегії кібербезпеки ЄС для цифрового десятиліття[5] (далі – Стратегія). Документ декларує прагнення ЄС забезпечити глобальний та відкритий Інтернет, який відповідатиме основним європейським цінностям. У положеннях Стратегії визначено три основні інструменти: регуляторний, інвестиційний і політичний, необхідні для досягнення цілей та низки відповідних завдань *(Рис.1)*.

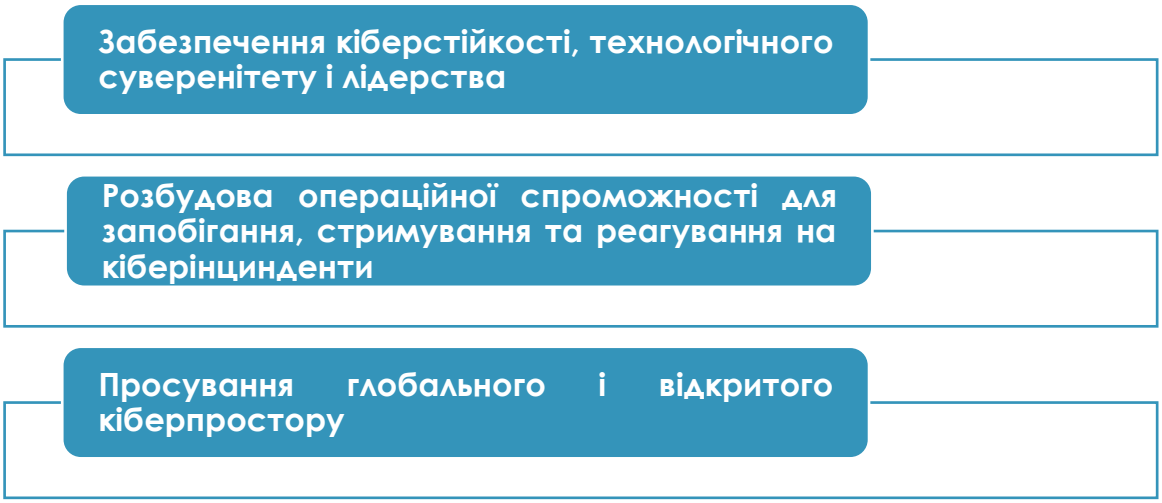

Рис. 1. Цілі Стратегії кібербезпеки ЄС для цифрового десятиліття

Такі амбітні цілі ґрунтуються на відповідному законодавчому забезпеченні. У цій площині ухвалено Регламент 2019/881 Європейського Парламенту і Ради від 17 квітня 2019 року про Агентство Європейського Союзу з кібербезпеки (далі – ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних

[3] Положення про організаційно-технічну модель кіберзахисту : Затверджено Постановою Кабінету Міністрів України від 29 грудня 2021 року № 1426. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text
[4] Національна система кібербезпеки функціонуватиме ефективніше. URL: https://cip.gov.ua/ua/news/nacionalna-sistema-kiberbezpeki-funkcionuvatime-efektivnishe
[5] Document 52020JC0018. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0018

технологій, а також скасування Регламенту (ЄС) № 526/2013[6] (далі – Регламент ЄС 2019/881), положення якого є обов'язковими для всіх держав-членів ЄС.

На відміну від попередніх актів ЄС про кібербезпеку, Регламент 2019/881 запровадив механізм забезпечення кібербезпеки за правилом стримування загроз за проектуванням інформаційних систем, а не за захистом і протидії загрозам. Це правило значною мірою стосується й публічних інформаційних систем.

Відповідно до приписів Регламенту 2019/881 створено уніфіковані для всіх держав-членів Європейські рамки сертифікації кібербезпеки, якими встановлено механізм для підтвердження того, що ІКТ-продукти, послуги та процеси відповідають визначеним вимогам безпеки з метою захисту доступності, автентичності, цілісності, конфіденційності збережених, переданих або оброблених даних, функцій, послуг, які пропонуються. Запроваджені Європейські рамки сертифікації кібербезпеки можуть визначати один або кілька таких рівнів надійності для ІКТ-продуктів, послуг і процесів: базовий, істотний, високий. Рівень достовірності повинен бути пропорційним рівню ризику, пов'язаного з передбачуваним використанням ІКТ-продукту, послуги або процесу, з точки зору ймовірності та впливу інциденту. Основні пріоритети Європейських рамок сертифікації кібербезпеки визначаються окремою робочою програмою.

Отже, Регламентом 2019/881 закріплений для всіх держав-членів ЄС уніфікований підхід щодо забезпечення кібербезпеки, який виходить з необхідності проектування електронних інформаційних ресурсів за принципом стримування кіберзагроз, відповідності міжнародним стандартам та європейським сертифікатам безпечності ІТ-продукції. Європейські схеми сертифікації кібербезпеки покликані допомогти гармонізувати практики кібербезпеки в ЄС.

Розвиваючи закладений Регламентом підхід до забезпечення кібербезпеки, 14 грудня 2022 року Рада ЄС затвердила Директиву (ЄС) 2022/2555 про заходи для високого загального рівня кібербезпеки в Союзі, внесення змін до Регламенту (ЄС) № 910/2014 і Директиви (ЄС) 2018/1972, а також про скасування Директиви (ЄС) 2016/1148[7] (далі – Директива NIS 2). Актом запроваджено заходи, спрямовані на досягнення високого загального рівня кібербезпеки в ЄС, з метою покращення функціонування внутрішнього ринку. Для досягнення цієї мети встановлені зобов'язання, які вимагають від держав-членів: прийняття національних стратегій кібербезпеки та планів реагування на масштабні інциденти та кризи в сфері кібербезпеки, а також призначення або створення компетентних органів – єдиних контактних пунктів з питань кібербезпеки і груп реагування на інциденти комп'ютерної безпеки; запровадження заходів з управління ризиками кібербезпеки та звітності для суб'єктів господарювання, чия діяльність пов'язана з управлінням критичною інфраструктурою;

[6] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj

[7] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

підвищення рівня кібербезпеки в ключових секторах економіки; обміну інформацією про кібербезпеку. 17 жовтня 2024 року сплив крайній строк для держав-членів щодо імплементації Директиви NIS 2.

Для діяльності ЄС у сфері забезпечення кібербезпеки, як правило, використовуються поняття «спільна політика кібербезпеки ЄС» або «екосистема політики кібербезпеки ЄС»[8], які реалізуються ENISA[9] (здійснює свою діяльність на підставі Регламенту ЄС 2019/881). Завданням ENISA є досягнення високого загального рівня кібербезпеки в Європі, сприяння реалізації політики ЄС з кібербезпеки, підвищення надійності ІКТ-продуктів, послуг і процесів за допомогою схем сертифікації кібербезпеки, налагодження співпраці з державами-членами та органами ЄС. ENISA кожні два роки подає звіт про стан кібербезпеки в ЄС Європейському парламенту. ENISA працює на двох рівнях *(Рис. 2)*:

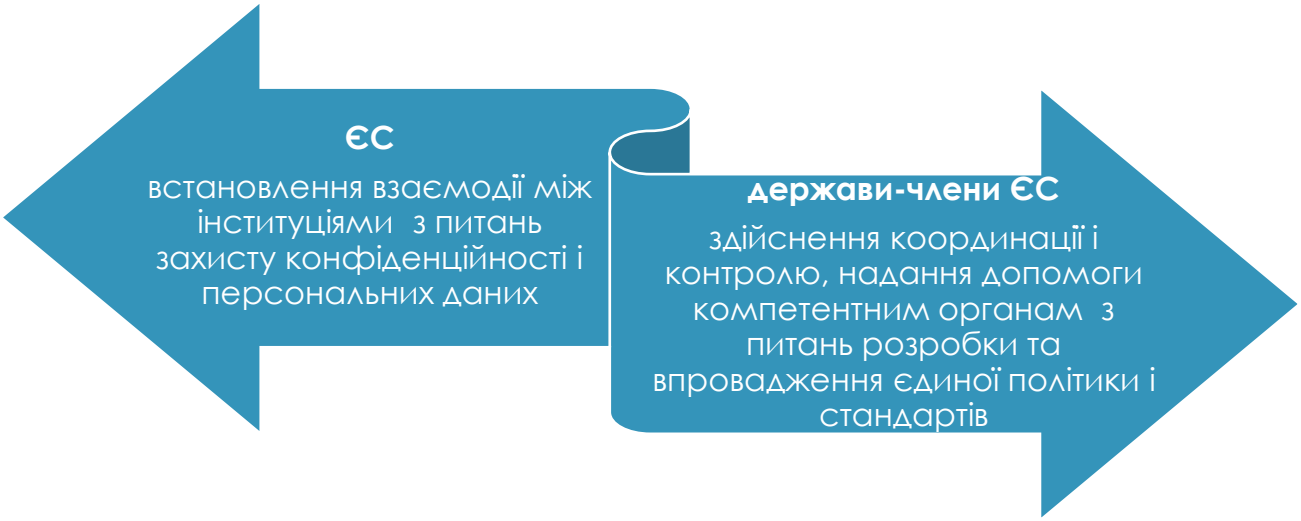

Рис. 2. Функціональні рівні ENISA

Очолює ENISA виконавчий директор. Контроль за діяльністю цієї інституції здійснюють виконавча рада і керівна рада, до складу яких входять представники держав-членів ЄС, Європейської комісії, інших зацікавлених сторін.

30 червня 2023 року Європейською Комісією закінчено 4-х етапний процес створення Об'єднаного кіберпідрозділу для реагування на масштабні кіберінциденти (далі – JCU)[10].

JCU є центральним координаційним підрозділом суб'єктів екосистеми політики кібербезпеки ЄС: ENISA, Команди реагування на комп'ютерні надзвичайні ситуації для інституцій, органів і агентств ЄС (CERT-EU), Європейського центру боротьби з кіберзлочинністю Європолу (EC3);

[8] Infographic: EU Cybersecurity Ecosystem. URL: https://digital-strategy.ec.europa.eu/en/library/infographic-eu-cybersecurity-ecosystem; Navigating the EU Cybersecurity Policy Ecosystem. URL: https://www.interface-eu.org/publications/navigating-the-eu-cybersecurity-policy-ecosystem

[9] The European Union Agency for Cybersecurit. Towards a Trusted and Cyber Secure Europe. Who we are. URL: https://www.enisa.europa.eu/about-enisa/who-we-are

[10] European Commission sets up a Joint Cyber Unit to respond to large-scale cyber incidents. URL: https://cyberwatching.eu/news-events/news/european-commission-sets-joint-cyber-unit-respond-large-scale-cyber-incidents; Joint Cyber Unit. URL: https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit

національних груп реагування на інциденти комп'ютерної безпеки (CSIRT), мережі організації зв'язку з кіберкризою ЄС (CyCLONE), Європейської служби зовнішніх дій (EEAS), Європейського оборонного агентства (EDA).

JCU здійснює такі види діяльності *(Рис. 3)*:

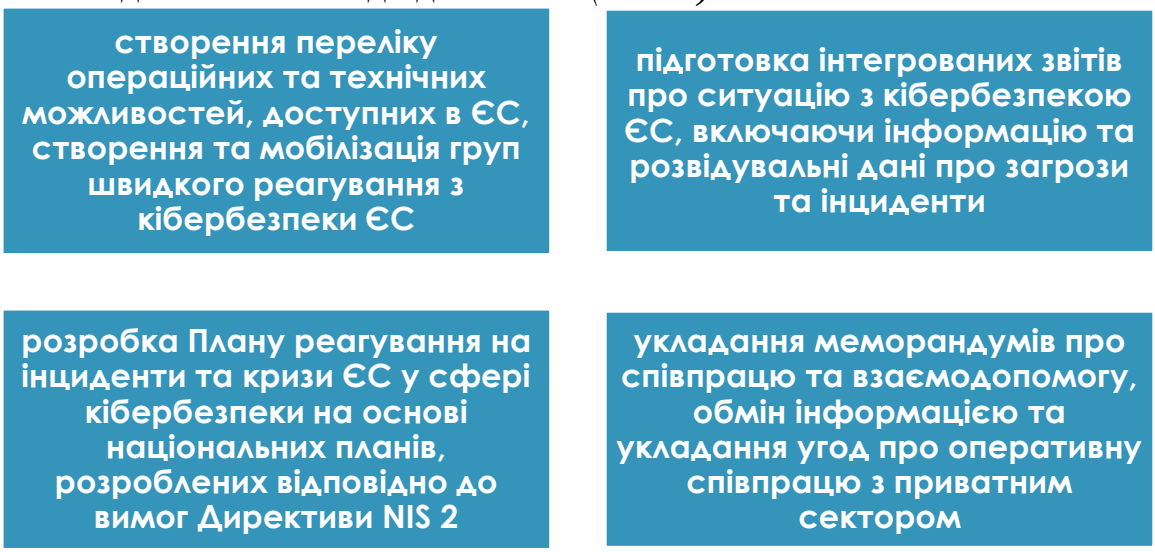

Рис. 3. Основні функції JCU

Упродовж останніх двох років Європейська комісія значно удосконалила правові інструменти, спрямовані на посилення екосистеми політики кібербезпеки ЄС. Зокрема, прийнято Регламент 2023/2841 Європейського Парламенту та Ради від 13 грудня 2023 року, що встановлює заходи для високого загального рівня кібербезпеки в установах, органах, офісах та агентствах Союзу[11] та Регламент (ЄС) 2024/2847 Європейського Парламенту та Ради від 23 жовтня 2024 року про горизонтальні вимоги до кібербезпеки для продуктів із цифровими елементами та внесення змін до Регламентів (ЄС) № 168/2013 та (ЄС) 2019/1020, та Директиви (ЄС) 2020/1828 (Закон про кіберстійкість (CRA)[12], спрямований на вирішення проблем неналежного рівня кібербезпеки цифрових продуктів або неадекватного оновлення їхньої безпеки шляхом встановлення граничних умов для розробки безпечних продуктів із цифровими елементами).

У процесі ухвалення перебуває регламент, що встановлюватиме заходи для посилення солідарності та потенціалу в Союзі для виявлення, підготовки і реагування на загрози кібербезпеці та інциденти (Закон про кіберсолідарність)[13]. Положеннями проекту передбачається створення Європейської системи оповіщення про кібербезпеку або так званого «європейського кіберщита», що

[11] Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union. URL: https://eur-lex.europa.eu/eli/reg/2023/2841

[12] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

[13] Document 52023PC0209. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023PC0209

складатиметься з операційних центрів безпеки (SOC), об'єднаних у кілька платформ. Передбачається, що SOC використовуватимуть передові технології на кшталт штучного інтелекту та аналітики даних задля виявлення й обміну попередженнями про кіберзагрози.

Політика у сфері кібербезпеки держав-членів ЄС базується на стандартах ЄС, відповідно до яких здійснюється прийняття національних стратегій кібербезпеки, планів реагування на масштабні інциденти та кризи. Створення національних органів або наділення відповідними повноваженнями існуючих органів є необхідністю.

У ***Латвії*** результатом реформи національної системи кібербезпеки стало прийняття Стратегії кібербезпеки Латвії на 2023 – 2026 роки[14] (далі – Стратегія) і Закону про національну кібербезпеку[15] (далі – NKDL).

Відповідно до Стратегії кібербезпека розглядається як елемент комплексної системи національної оборони, саме тому завданням Міністерства оборони Латвійської Республіки є створення і реалізація політики кібербезпеки в державі.

Відповідно до положень NKDL структура нової моделі системи управління кібербезпекою передбачає створення Національного центру кібербезпеки[16], який виконуватиме функції контактного органу з питань кібербезпеки, здійснюватиме нагляд за виконанням вимог кібербезпеки, формуватиме національну політику кібербезпеки (стаття 4). Функції Національного центру кібербезпеки виконуватиме Міністерство оборони Латвійської Республіки у співпраці з Інститутом запобігання кіберінцидентів (CERT.LV). Останній відповідатиме за реагування на інциденти кібербезпеки, моніторинг ситуації в кіберпросторі та аналіз загроз, забезпечення роботи сенсорної мережі, брандмауера DNS і операційних центрів безпеки, навчання громадськості з питань кібербезпеки.

До структури системи управління кібербезпекою входять: Управління конституційного захисту (орган нагляду за критичною інфраструктурою інформаційно-комунікаційних технологій) (стаття 7); Національна рада з кібербезпеки[17] (дорадчий орган з координації розробки політики, пов'язаної з кібербезпекою, планування та виконання відповідних завдань і заходів) (стаття 16); установи, які надають державним установам та органам місцевого самоврядування підтримку у сфері кібербезпеки.

Завдання установ із запобігання кіберінцидентам виконують: Служба військової розвідки та безпеки (щодо Міністерства оборони, підпорядкованих йому установ і Національних Збройних Сил); Інститут математики та інформатики Латвійського університету (щодо державних установ, установ місцевого самоврядування, юридичних осіб приватного права (стаття 9)).

---

[14] Par Latvijas kiberdrošības stratēģiju 2023.–2026. gadam. Ministru kabineta rīkojums № 158 Rīgā 2023. gada 28. martā. URL: https://likumi.lv/ta/id/340633-par-latvijas-kiberdrosibas-strategiju-20232026-gadam

[15] Nacionālās kiberdrošības likums. URL: https://likumi.lv/ta/id/353390-nacionalas-kiberdrosibas-likums

[16] Saeima pieņem Nacionālās kiberdrošības likumu. URL: https://lvportals.lv/dienaskartiba/364994-saeima-pienem-nacionalas-kiberdrosibas-likumu-2024

[17] Par Nacionālo kiberdrošības padomi. Ministru prezidenta rīkojums № 2024/1.2.1.-416 Rīgā 2024. gada 6. Decembrī. URL: https://likumi.lv/ta/id/357025-par-nacionalo-kiberdrosibas-padomi

Юридичні особи, що працюють в державі, повинні оцінити свою діяльність у контексті того чи є вони постачальниками відповідних послуг або ж власниками критичної інфраструктури інформаційно-комунікаційних технологій у розумінні NKDL. У разі відповідності вимогам NKDL зазначені особи зобов'язані до 1 квітня 2025 року надіслати реєстраційну форму до Національного центру кібербезпеки на електронну адресу Міністерства оборони Латвійської Республіки, призначити менеджера з кібербезпеки і подати звіт про самооцінку (до 1 жовтня 2025 року). Законодавством також визначені вимоги щодо звітування про інциденти і виявлені вразливості, розробки плану управління ризиками.

У ***Польщі*** у 2018 році було прийнято Закон про національну систему кібербезпеки[18], на реалізацію якого Радою міністрів було затверджено Стратегію кібербезпеки Республіки Польща на 2019-2024 роки[19].

Стратегією визначено п'ять конкретних цілей державної політики з кібербезпеки, зокрема щодо розвитку національної системи кібербезпеки і підвищення рівня стійкості інформаційних систем державного управління та приватного сектору, ефективного запобігання інцидентам і реагування на них.

Відповідно до Закону про національну систему кібербезпеки[20] метою національної системи кібербезпеки (далі – KSC) є її забезпечення на національному рівні – гарантування безперебійного надання відповідних послуг і досягнення високого рівня безпеки систем ІКТ, які використовуються для надання цих послуг. Завданням KSC є виявлення, запобігання та мінімізації наслідків атак, які порушують безпеку важливих для функціонування держави інформаційних систем. Крім того, відповідно до законодавства KSC посилює взаємодію між різними суб'єктами стосовно обміну інформацією про загрози та координації дій у разі виникнення інцидентів.

KSC охоплюють низку секторів, які вважаються ключовими для функціонування держави та економіки: енергетичний (виробництво, передача, розподіл і зберігання електроенергії, сирої нафти та природного газу); транспортний (повітряний, залізничний, водний та автомобільний транспорт); банківський (банки, кредитні установи, інвестиційні компанії, страхові компанії, тощо); охорони здоров'я (медичні установи, аптеки, фармацевтичні оптові торговці); постачання та розподілу питної води; цифрової інфраструктури (точки обміну Інтернетом (IXP), постачальники послуг (DNS), реєстри доменних імен верхнього рівня); державного управління (органи державної влади та органи місцевого самоврядування).

Основними суб'єктами є: оператори ключових послуг (суб'єкти, які надають послуги і мають ключове значення для підтримки критичної соціальної чи економічної діяльності); постачальники цифрових послуг (організації, що надають цифрові послуги, зокрема онлайн-ринки, послуги хмарних обчислень

[18] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. URL: https://www.dziennikustaw.gov.pl/DU/rok/2018/pozycja/1560

[19] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Wersja od: 10 listopada 2024 r. URL: https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/krajowy-system-cyberbezpieczenstwa-18746756

[20] Czym jest Krajowy System Cyberbezpieczeństwa – Najważniejsze informacje. URL: https://nflo.pl/baza-wiedzy/czym-jest-krajowy-system-cyberbezpieczenstwa-najwazniejsze-informacje/

або онлайн-пошукові системи); CSIRT (Computer Security Incident Response Teams, далі– CSIRT) на національному рівні (групи, відповідальні за розгляд інцидентів на національному рівні); секторальні команди кібербезпеки (групи, створені для конкретних економічних секторів, які підтримують операторів ключових послуг у певному секторі); суб'єкти, які надають послуги з кібербезпеки (компанії, що пропонують пов'язані з кібербезпекою послуги); органи, що відповідають за кібербезпеку (органи державної влади). KSC також є центром співпраці органів державного управління (Агентство внутрішньої безпеки, поліція, Урядовий центр безпеки, Національний центр кібербезпеки) з телекомунікаційним сектором. CSIRT виконують основну функцію, оскільки є першою точкою контакту для організацій, які повідомляють про інциденти та координують діяльність, пов'язану з реагуванням на загрози національного рівня. Таких команд є три: CSIRT GOV (керується керівником Агентства внутрішньої безпеки, відповідальним за координацію обробки інцидентів, про які повідомляє державна адміністрація, оператори критичної інфраструктури, а також власники об'єктів критичної інфраструктури); CSIRT NASK (керується Науковою та академічною комп'ютерною мережею (NASK), відповідальною за обробку інцидентів, про які повідомляють інші організації, зокрема оператори ключових послуг, постачальники цифрових послуг, малі та середні підприємства, та окремі особи); CSIRT Міністерства національної оборони Республіки Польща (керується міністром національної оборони, відповідальним за розгляд інцидентів, про які повідомляють організації, підпорядковані або підконтрольні Міністерству).

Управління структурою KSC[21] здійснює уряд, який визначає стратегічні напрями політики кібербезпеки та контролює її реалізацію. Міністр з цифрових питань координує діяльність на оперативному рівні; Урядовий уповноважений з кібербезпеки (призначається Прем'єр-міністром) відповідає за координацію політики кібербезпеки та нагляд за функціонуванням KSC; Коледж кібербезпеки є консультативно-дорадчим органом з питань кібербезпеки (до складу входять представники провідних міністерств, спецслужб і зовнішні експерти); Єдина контактна точка або Єдиний контактний пункт (PPK) (підпорядковується міністру з питань цифровізації) забезпечує ефективний обмін інформацією і координує співпрацю у сфері кібербезпеки на рівні ЄС.

На операційному рівні управління здійснюють міністри, відповідальні за окремі сектори економіки, які взаємодіють з групами CSIRT, а ті, в свою чергу, тісно співпрацюють з ключовими операторами послуг, постачальниками цифрових послуг та іншими суб'єктами, залученими до кібербезпеки.

Також важливо відмітити, що національні стандарти кібербезпеки, які діють у польській правовій системі (NSC)[22], розроблені на основі практики федеральної адміністрації США та NIST.

[21] Jak zorganizowany jest Krajowy System Cyberbezpieczeństwa? Kompleksowy przewodnik po strukturze i funkcjonowaniu polskiego systemu ochrony cyberprzestrzeni. URL: https://nflo.pl/baza-wiedzy/jak-zorganizowany-jest-krajowy-system-cyberbezpieczenstwa-kompleksowy-przewodnik-po-strukturze-i-funkcjonowaniu-polskiego-systemu-ochrony-cyberprzestrzeni/

[22] Narodowe Standardy Cyberbezpieczeństwa. URL: https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber

Румунія також оновлює національне законодавство у сфері кібербезпеки. Так 28 грудня 2018 року прийнято Закон про забезпечення загального високого рівня безпеки мереж та IT-систем[23], а 14 березня 2023 року – Закон про безпеку та кіберзахист Румунії та про внесення змін та доповнень до деяких нормативних актів (далі – Закон про кіберзахист)[24].

Завдання і структура органів, залучених до організації національної системи кібербезпеки Румунії (далі – SNSC), визначені у положеннях Закону про кіберзахист. SNSC має трьохрівневу структуру (*Рис. 4):*

Рис. 4. Рівні SNSC в Румунії

На оперативному рівні діє COSC, до складу якого входить радник Президента з питань національної безпеки, радник Прем'єр-міністра з питань національної безпеки, секретар CSAT, а також представники міністерств (національної оборони, внутрішніх справ, закордонних справ, досліджень, інновацій та цифровізації), Служби зовнішньої розвідки, Спеціальної служби телекомунікацій, Служби захисту та охорони, Офісу Національного реєстру державної таємниці, Національного управління з адміністрування та регламенту у сфері комунікацій, Національного директорату з кібербезпеки. Як дорадчий орган він видає консультативні висновки та рекомендації, ухвалені консенсусом. COSC співпрацює, у разі необхідності, з координаційними або управлінськими органами, створеними на національному рівні для управління надзвичайними ситуаціями, дій у кризових ситуаціях у сфері громадського порядку, запобігання та боротьби з тероризмом, забезпечення безпеки та національної оборони.

Діяльність COSC технічно забезпечує SRI, який є національним органом, що здійснює функції з аналізу, запобігання та протидії інцидентам і кібератакам, які представляють загрози і ризики для національної безпеки Румунії.

Всі органи, представники яких входять до складу COSC, діють у межах своїх секторальних повноважень. До прикладу, Служба зовнішньої розвідки (SIE) є компетентним органом для визначення, аналізу, запобігання та протидії кіберінцедентам і атакам, які представляють кіберзагрози для мереж і IT-систем, що знаходяться в його відповідальності. Служба захисту та охорони (SPP) є компетентним органом у сфері кібербезпеки для своїх власних інфраструктур,

[23] LEGE nr. 362 din 28 decembrie 2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice. URL: https://legislatie.just.ro/Public/DetaliiDocumentAfis/245744

[24] LEGE nr. 58 din 14 martie 2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative URL: https://legislatie.just.ro/Public/DetaliiDocument/265677

мереж, систем і послуг, яка координує заходи кібербезпеки для високопосадовців, яким надає захист, і діє незалежно або у співпраці з іншими структурами у сферах оборони, громадського порядку та національної безпеки, для їх реалізації. Національний реєстр державної таємниці (ORNISS) координує діяльність, що здійснюється з метою забезпечення кібербезпеки мереж і комп'ютерних систем, які зберігають, обробляють або передають секретну інформацію.

Також в державі функціонує Національний директорат з кібербезпеки – спеціалізований державний орган (координує діяльність Прем'єр-міністр), який фінансується з державного бюджету через бюджет Секретаріату уряду і діє відповідно до положень Надзвичайної урядової постанови[25].

Відповідно до вимог Директиви ЄС NIS2 в органах державної влади, установах, інших юридичних особах створені і діють групи реагування на інциденти кібербезпеки (CSIRT) – спеціалізовані організаційні одиниці з необхідним потенціалом для запобігання, аналізу, ідентифікації та реагування на кіберінциденти.

Модель кібербезпеки ***Ізраїлю*** основана на новітніх технологіях і створенні правових механізмів для захисту інформаційної інфраструктури[26]. Це пояснюється високим розвитком IT-технологій і необхідністю збереження державності. Так у Звіті за 2024 рік[27], оприлюдненому Загальною службою безпеки Ізраїлю, вказується на 5-кратне збільшення кількості кібератак протягом військової кампанії під кодовою назвою «Операція «Залізні мечі»[28] з 7 жовтня 2023 року.

Регулювання інформаційної безпеки Ізраїлю ґрунтується на законодавстві, яке охоплює широкий спектр нормативно-правових актів, зокрема закони: про захист приватного життя[29], про комп'ютери[30], про заохочення досліджень, розробок і технологічних інновацій у промисловості[31], про комунікації (телекомунікації та радіомовлення)[32], про експортний контроль оборонної промисловості[33], про боротьбу з тероризмом. Значний вплив на

---

[25] ORDONANȚĂ DE URGENȚĂ nr. 104 din 22 septembrie 2021 privind înființarea Directoratului Național de Securitate Cibernetică. URL: https://legislatie.just.ro/Public/DetaliiDocumentAfis/262595

[26] Дзеньків В. Кібербезпека в умовах сучасних загроз: Ізраїльський досвід та його застосування в Україні. *Науковий вісник Ужгородського Національного Університету*, 2024. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/09/14-2.pdf

[27] חושף כ"השב ח"דו :סגולה יחידי נחלת" עוד אינו סייבר סיכוני ניהול URL: https://hay-law.com/%D7%93%D7%95%D7%97-%D7%94%D7%A9%D7%91%D7%9B-%D7%97%D7%95%D7%A9%D7%A3-%D7%A0%D7%99%D7%94%D7%95%D7%9C-%D7%A1%D7%99%D7%9B%D7%95%D7%A0%D7%99-%D7%A1%D7%99%D7%99%D7%91%D7%A8-%D7%90%D7%99%D7%A0%D7%95/

[28] Абрамова Ю. Операція Ізраїлю «Залізні мечі» стане «неперевершеною за своєю жорстокістю» – експерти про майбутній наступ. URL: https://tsn.ua/svit/operaciya-izrayilyu-zalizni-mechi-stane-nepereversheno yu-za-svoyeyu-zhorstokistyu-eksperti-pro-maybutniy-nastup-2433106.html

[29] חוק הגנת הפרטיות, תשמ"א-1981. URL: https://www.nevo.co.il/law_html/law00/71631.htm

[30] חוק המחשבים, תשנ"ה-1995. URL: https://www.nevo.co.il/law_html/law00/72393.htm

[31] חוק לעידוד מחקר, פיתוח וחדשנות טכנולוגית בתעשיה, תשמ"ד-1984. URL: https://www.nevo.co.il/law_html/law01/p181m2_001.htm

[32] חוק התקשורת (בזק)(חוק ושידורים) URL: https://www.kolzchut.org.il/he/%D7%97%D7%95%D7%A7_%D7%94%D7%AA%D7%A7%D7%A9%D7%95%D7%A8%D7%AA_(%D7%91%D7%96%D7%A7_%D7%95%D7%A9%D7%99%D7%93%D7%95%D7%A8%D7%99%D7%9D)

[33] חוק הפיקוח על יצוא ביטחוני, תשס"ז-2007. URL: https://www.nevo.co.il/law_html/law01/999_796.htm

формування політики у сфері кібербезпеки мають правила, розроблені неурядовими організаціями щодо надання інтернет-послуг[34].

Основою організації системи національної кібербезпеки є Закон про регулювання безпеки в державних органах[35], яким врегульовано питання контролю і нагляду за діяльністю органів, що уповноваженні здійснювати керівництво основними комп'ютеризованими системами держави, а також Рішення уряду про розвиток національного потенціалу в кіберпросторі[36].

У результаті реформування і модернізації національної системи кібербезпеки у 2018 році функції національного координатора у сфері кіберзахисту, які з 2002 року виконувало Національне управління з інформаційної безпеки (NISA) у межах Загальної служби безпеки Ізраїлю[37], інтегровані до Ізраїльського національного кібердиректорату (далі–INCD)[38], створеного при Офісі Прем'єр-міністра. Такий перерозподіл повноважень дозволив забезпечити ефективний захист кіберпростору. INCD є органом до повноважень якого віднесено забезпечення кібероборони в цивільному секторі.

До структури INCD входить Команда реагування на кібернетичні ситуації (далі–CERT)[39]. Функціями CERT є: реагування на кіберінциденти; здійснення профілактичних заходів у сфері кіберзахисту; координацію зв'язків між провідними галузями економіки, урядом і міжнародними партнерами; покращення обміну інформацією тощо. До складу CERT входить Національний центр управління інцидентами і чотири галузеві центри. Національний центр управління інцидентами здійснює постійний моніторинг кіберзагроз (розробляє стандарти і рекомендації щодо можливостей врегулювання кіберінцидентів, як в приватному, так і в державному секторах). Галузеві центри створені INCD у співпраці з профільними міністерствами. Згадані центри пропонують професійні рішення щодо подолання кіберзагроз у конкретних секторах.

Крім того, до складу національної системи кібербезпеки включено низку спеціальних органів, зокрема: Армію оборони Ізраїлю (у складі функціонують кібервійська під управлінням кіберкомандування), Ізраїльську поліцію, Службу загальної безпеки, Інститут розвідки та спеціальних обов'язків і установи безпеки[40].

Для забезпечення повноцінної та ефективної системи кібербезпеки уряд Ізраїлю ініціює і підтримує програми навчання спеціальних кадрів, а також інформаційні програми для населення країни, наприклад, навчання школярів

---

[34] Бєлєвцева В.В. Основи правового регулювання інформаційної сфери у державі Ізраїль. *Інформація і право.* № 1(48), (2024). URL: http://il.ippi.org.ua/article/view/300802

[35] חוק להסדרת הבטחון בגופים ציבוריים, תשנ"ח-1998. URL: https://www.nevo.co.il/law_html/law00/71736.htm

[36] הקיברנטי במרחב הלאומית היכולת קידום URL: https://www.gov.il/he/pages/2011_des3611

[37] ציבורים בגופים הביטחון להסדרת והחוק הממשלה החלטות URL: https://www.gov.il/he/pages/govdecisions

[38] Israel National Cyber Directorate. URL: https://www.gov.il/en/pages/newabout; דרעמ רבייסה ימואלה 3. תפסוה תרשמ שאר תוריש הנידמה (סייונימ) 4. תעיבק רכש יאנתו תוריש לש שאר דרעמ 1. דוחיא תודיחי דרעמ רבייסה ימואלה 2. וחמ רוטפ זרכממ תרשמל שאר רפסמ הטלחה: 3270 רבייסה ימואלה דרעמ רבייסה ימואלה תפסותל יפל חיעס 23 קוחל URL: https://www.gov.il/BlobFolder/news/govdecisions/he/3270.pdf

[39] The Israeli Cyber Emergency Response Team (CERT). URL: https://www.gov.il/en/pages/119en

[40] מיום הממשלה של 3611 מס. החלטה הקיברנטי במרחב הלאומית היכולת קידום .07.08.2011 URL: https://www.gov.il/he/pages/2011_des3611

навичкам цифрового захисту. Крім того, в державі підтримується кілька освітніх програм для молоді віком 16-18 років[41].

До співпраці у сфері забезпечення кібербезпеки активно залучаються компанії приватного сектору.

У 2024 році уряд ***Південної Кореї*** затвердив оновлену Національну стратегію кібербезпеки[42] (далі – Стратегія) і визначив Північну Корею стратегічною загрозою кібербезпеки. У розвиток положень Стратегії урядом затверджено Національний базовий план кібербезпеки[43], який запроваджує низку заходів.

Указом Президента про правила управління кібербезпекою[44] (далі – Правила) визначено структуру національної системи кібербезпеки. Координуючим органом визначено Управління національної безпеки (NSO) при Президенті, а базовим органом, який здійснює оперативне управління на національному рівні – Національну службу розвідки (далі–NIS), обов'язком якої, відповідно до положень Закону про Національну розвідувальну службу[45], є запобігання та реагування на кібератаки та кіберзагрози на національному рівні. NIS уповноважена здійснювати нагляд і координувати державну політику у сфері кібербезпеки у взаємодії з керівниками відповідних центральних органів державної влади. У складі NIS функціонують Директорат, Рада з питань стратегії національної кібербезпеки, Національна рада з питань протидії кіберзагрозам, Національний центр кібербезпеки.

Рада з питань стратегії національної кібербезпеки і Національна рада з питань протидії кіберзагрозам є дорадчими колегіальними органами, до складу яких входять представники профільних міністерств і відомств.

Рада з питань стратегії національної кібербезпеки відповідальна за підготовку і вдосконалення національної стратегії кібербезпеки, а також розгляд питань, пов'язаних з державною політикою кібербезпеки та координацією міжвідомчих зв'язків. Національна рада з питань протидії кіберзагрозам зосереджується на розгляді питань щодо управління кібербезпекою та протидії кіберзагрозам тощо.

---

[41] Гребенюк М. В., Леонов Б. Д. Досвід Ізраїлю у сфері забезпечення кібербезпеки. *Інформація і право.* № 2(25)/2018. URL: https://ippi.org.ua/sites/default/files/6_9.pdf

[42] South Korean National Cybersecurity Strategy URL: https://dig.watch/resource/south-korean-national-cybersecurity-strategy

[43] 국가안보실이 발표한 '국가 사이버안보 기본계획'... 어떤 내용 담겼나 URL: https://m.boannews.com/html/detail.html?idx=132475#:~:text='%EA%B5%AD%EA%B0%80%EC%82%AC%EC%9D%B4%EB%B2%84%EC%95%88%EB%B3%B4%20%EA%B8%B0%EB%B3%B8%EA%B3%84%ED%9A%8D'%EC%9D%80%20%EC%A7%80%EB%82%9C%202%EC%9B%94%201,%EC%97%85%EB%AC%B4%20%EC%88%98%ED%96%89%EA%B8%B0%EB%B0%98%20%EA%B0%95%ED%99%94%EC%9D%B4%EB%8B%A4

[44] 국가사이버안전관리규정 URL: https://www.law.go.kr/%ED%96%89%EC%A0%95%EA%B7%9C%EC%B9%99/%EA%B5%AD%EA%B0%80%EC%82%AC%EC%9D%B4%EB%B2%84%EC%95%88%EC%A0%84%EA%B4%80%EB%A6%AC%EA%B7%9C%EC%A0%95

[45] 국가정보원법

URL: https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B5%AD%EA%B0%80%EC%A0%95%EB%B3%B4%EC%9B%90%EB%B2%95

У цьому контексті варто відмітити, що директор NIS уповноважений окремо доручати керівникам центральних органів державної влади і місцевого самоврядування впроваджувати заходи кібербезпеки.

У складі NIS функціонує Національний центр кібербезпеки, до повноважень якого віднесено: формування національної політики кібербезпеки; збір, аналіз і розповсюдження інформації про кіберзагрози; забезпечення безпеки національної інформаційно-комунікаційної мережі; підготовку національного посібника з кібербезпеки; розслідування випадків кібератак; співпрацю з іноземними державами у сфері інформації, пов'язаної з кіберзагрозами тощо.

Оскільки профільні міністерства і відомства залучені до виконання завдань у межах національної системи кібербезпеки, то вони уповноважені здійснювати діяльність у сфері кібербезпеки і захисту інформації відповідно й до норм галузевого законодавства. Зокрема, діяльність у цій сфері регулюється законами: про електронні фінансові операції[46], про сприяння використанню інформаційно-комунікаційних мереж і захисту інформації[47], про охорону здоров'я та медичні послуги[48], про управління транспортними засобами[49], про створення інформаційної інфраструктури оборони та управління інформаційними ресурсами оборони[50] тощо.

Нові пріоритети кібербезпеки ***США*** оприлюднено у Національній стратегії кібербезпеки[51]. У положеннях акта Китай і Росія визначаються як найбільш серйозні загрози державній кібербезпеці. У зв'язку з цим визначено п'ять стратегічних цілей забезпечення національної безпеки США у кіберпросторі *(Рис.5)*.

---

[46] 전자금융거래법 URL: https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%84%EC%9E%90%EA%B8%88%EC%9C%B5%EA%B1%B0%EB%9E%98%EB%B2%95

[47] 정보통신망 이용촉진 및 정보보호 등에 관한 법률 URL: https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EB%A7%9D%EC%9D%B4%EC%9A%A9%EC%B4%89%EC%A7%84%EB%B0%8F%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%93%B1%EC%97%90%EA%B4%80%ED%95%9C%EB%B2%95%EB%A5%A0

[48] 보건의료기본법 URL: https://www.law.go.kr/LSW/lsInfoP.do?lsId=002029#0000

[49] 자동차관리법 URL: https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%9E%90%EB%8F%99%EC%B0%A8%EA%B4%80%EB%A6%AC%EB%B2%95

[50] 국방정보화 기반조성 및 국방정보자원관리에 관한 법률URL: https://casenote.kr/%EB%B2%95%EB%A0%B9/%EA%B5%AD%EB%B0%A9%EC%A0%95%EB%B3%B4%ED%99%94_%EA%B8%B0%EB%B0%98%EC%A1%B0%EC%84%B1_%EB%B0%8F_%EA%B5%AD%EB%B0%A9%EC%A0%95%EB%B3%B4%EC%9E%90%EC%9B%90%EA%B4%80%EB%A6%AC%EC%97%90_%EA%B4%80%ED%95%9C_%EB%B2%95%EB%A5%A0/%EC%A0%9C2%EC%A1%B0#:~:text=%22%EA%B5%AD%EB%B0%A9%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%22%EB%9E%80%20%EA%B5%AD%EB%B0%A9,%EC%9C%84%ED%95%9C%20%EB%AA%A8%EB%93%A0%20%ED%99%9C%EB%8F%99%EC%9D%84%20%EB%A7%90%ED%95%9C%EB%8B%A4.

[51] The US has announced its National Cybersecurity Strategy: Here's what you need to know. URL: https://www.weforum.org/stories/2023/03/us-national-cybersecurity-strategy/

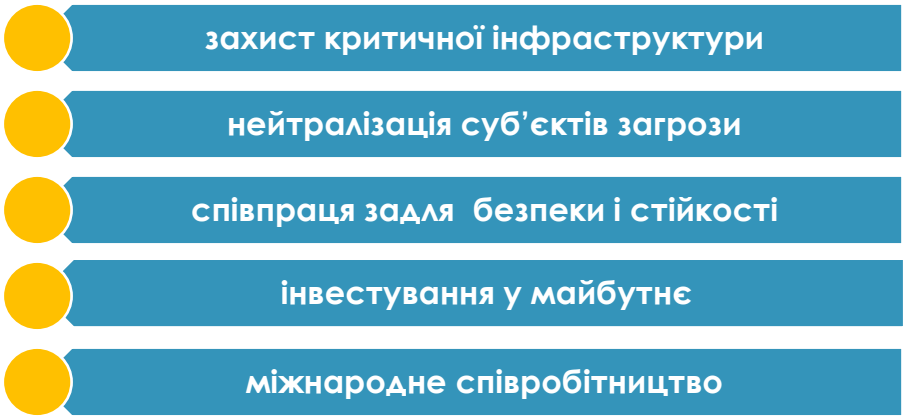

Рис. 5. Ключові цілі Національної стратегії кібербезпеки США

Загальнодержавний підхід до реалізації Національної стратегії кібербезпеки США координує Офіс Національного кібердиректора (ONCD)[52], який є складовою виконавчого офісу Президента в Білому домі, здійснює консультативну функцію щодо політики та стратегії кібербезпеки.

Стратегічні цілі державної політики США у сфері кібербезпеки ґрунтуються на достатньо розгалуженому й об'ємному законодавстві. Наразі в США відсутній федеральний закон про кібербезпеку[53]. Деякі федеральні закони, прийняті з метою врегулювання кібербезпекових питань є галузевими або поширюються лише на публічні компанії. До прикладу, Законом про цінні папери[54] переслідується шахрайство, а Комісія з цінних паперів і бірж (SEC) дотримується вимог щодо належного публічного розкриття інформації у контексті кібербезпеки. Закон про медичне страхування (HIPAA)[55] містить вимоги щодо кібербезпеки, які застосовуються до захищеної медичної інформації, якою володіють певні організації та їхні партнери.

Попри відсутність єдиного федерального закону про кібербезпеку, правова основа для формування державної політики щодо захисту кіберпростору та державних інформаційних ресурсів задля забезпечення інтересів національної безпеки визначена у Національній доктрині кібербезпеки США (CNCI)[56] і відповідних законах, зокрема: про комп'ютерне шахрайство та зловживання (CFAA)[57] (запроваджує механізм переслідування кіберзлочинів); про конфіденційність електронних комунікацій (ECPA)[58] (забезпечує захист зв'язку під час зберігання та передачі); про покращення кібербезпеки Інтернету речей в США (шляхом підвищення кібербезпеки для пристроїв Інтернету речей)[59]; про

[52] Office of the National Cyber Director, The White House. URL: https://www.linkedin.com/company/cyberdirector/
[53] Cybersecurity Laws and Regulations USA 2025. URL: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa
[54] 15 U.S. Code Chapter 2A - SECURITIES AND TRUST INDENTURES. URL: https://www.law.cornell.edu/uscode/text/15/chapter-2A
[55] Health Insurance Portability and Accountability Act of 1996 (HIPAA). URL: https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html
[56] NATIONAL SECURITY PRESIDENTIAL DIRECfiVEINSPD-54. HOMELAND SECURITY PRESIDENTIAL DIRECTNE/HSPD-23. URL: https://irp.fas.org/offdocs/nspd/nspd-54.pdf
[57] 18 U.S. Code § 1030-Fraud and related activity in connection with computers. URL: https://www.law.cornell.edu/uscode/text/18/1030
[58] Electronic Communications Privacy Act of 1986 (ECPA). URL: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285
[59] H.R.1668 - IoT Cybersecurity Improvement Act of 2020. 116th Congress (2019-2020). URL: https://www.congress.gov/bill/116th-congress/house-bill/1668/text

обмін даними про кіберрозвідку і захист (шляхом посиленого обміну інформацією про загрози кібербезпеці)[60]; про агентство з кібербезпеки та безпеки інфраструктури (далі–CISA)[61]; про звітність про кіберінциденти щодо критичної інфраструктури (CIRCIA).

Організація і здійснення кіберзахисту на федеральному рівні покладена на CISA (Cybersecurity and Infrastructure Security Agency) – Федеральне агентство у складі Департаменту (міністерства) внутрішньої безпеки (далі – DHS)[62], відповідальне за забезпечення кібербезпеки та захист критичної інфраструктури. CISA виконує дві основні операційні функції *(Рис.6):*

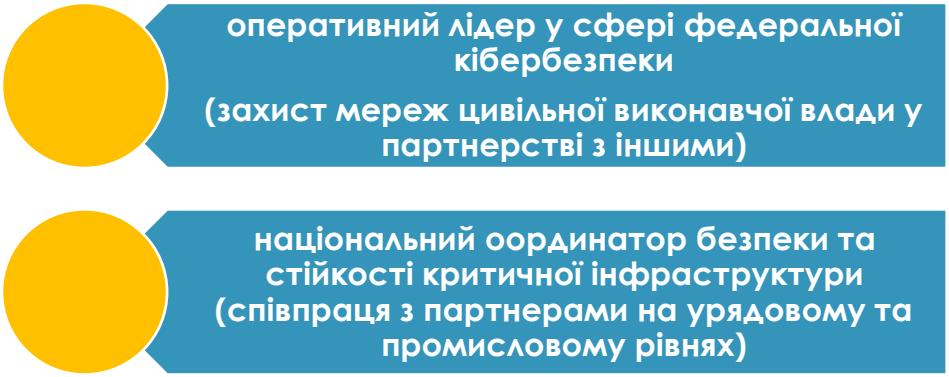

Рис.6. Основні операційні функції CISA

На офіційному вебсайті CISA[63] надано визначення поняття «національна система захисту кібербезпеки» (далі – NCPS) та представлено її структуру.

Технологією CISA в NCPS є виявлення вторгнень (EINSTEIN)[64], яка є інструментом захисту федеральної мережі.

Рада з аналізу кібербезпеки (далі – CSRB) – державно-приватний консультативний орган, який об'єднує кіберекспертів державного і приватного секторів задля здійснення аналізу щодо найбільш значущих кіберінцидентів.

Висновки.

Аналіз законодавства окремих держав свідчить про пріоритетність питання забезпечення захисту кіберпростору та державних інформаційних ресурсів для їх національної безпеки. З початку повномасштабної війни російської федерації проти України держави суттєво оновили законодавство і удосконалили національні системи кібербезпеки, оскільки кіберзлочинність нарощує потенціал впливу на перебіг збройних конфліктів, доповнюючи традиційні форми ведення війни. На прикладі таких держав-членів ЄС як Латвія, Польща, Румунія, а також Південна Корея і США прослідковується тенденція до прийняття принципово

[60] H.R.3523 - Cyber Intelligence Sharing and Protection Act. 112th Congress (2011-2012). URL: https://www.congress.gov/bill/112th-congress/house-bill/3523

[61] 6 U.S. Code § 652 - Cybersecurity and Infrastructure Security Agency. URL: https://www.law.cornell.edu/uscode/text/6/652

[62] Cybersecurity. The Department of Homeland Security. URL: https://www.dhs.gov/topics/cybersecurity

[63] National Cybersecurity Protection System. URL: https://www.cisa.gov/resources-tools/programs/national-cybersecurity-protection-system

[64] EINSTEIN. URL: https://www.cisa.gov/resources-tools/programs/national-cybersecurity-protection-system/einstein

нових або суттєво удосконалених національних стратегій і законодавства про кібербезпеку з огляду на війну в Україні. Зокрема, у Національній стратегії кібербезпеки США Китай і Росія визначаються як найбільш серйозні загрози кібербезпеці, тому значно посилюється відповідальність держави щодо захисту кіберпростору. У Національній стратегії кібербезпеки Південної Кореї стратегічною загрозою визначено Північну Корею.

Варто зазначити, що моделі побудови національних систем кібербезпеки мають певні спільні риси. Як правило, структура управління системами кібербезпеки має трирівневу архітектоніку і свідчить про домінантну роль безпекових, розвідувальних чи контррозвідувальних служб у забезпеченні кібербезпеки на оперативному рівні. Такий підхід об'єктивно пояснюється характером кіберзагроз, протидія яким потребує спеціального інструментарію, яким оперують виключно відповідні державні органи.

Стратегічні позиції в управлінні національними системами кібербезпеки зазвичай займають колегіальні органи (на чолі з прем'єр-міністром або президентом), до складу яких обов'язково входять міністри, відповідальні за певні галузі критичної інфраструктури (оборонної, енергетичної, транспортної, банківської, інформаційних технологій та електронних комунікацій, продовольства, охорони здоров'я).

На оперативному та технічному рівнях до участі у здійсненні заходів, пов'язаних з виявленням, запобіганням і нейтралізацією кіберзагроз, залучаються інші суб'єкти забезпечення кібербезпеки. Іноді оперативний і технічний рівні можуть бути об'єднані та забезпечуватись одним суб'єктом.

Уніфіковану модель системи кібербезпеки вироблено в ЄС. Сутність політики кібербезпеки ЄС полягає у встановленні та впровадженні чітких правил, які визначають колективну здатність держав-членів ЄС і ЄС запобігати, виявляти, стримувати, відповідати на кіберзагрози та кібератаки. На виконання задекларованих цілей політики кібербезпеки впродовж останніх років Єврокомісія впровадила низку ініціатив, зокрема щодо підвищення рівня кібербезпеки в державах-членах ЄС; встановлення спільних стандартів кібербезпеки для інституцій ЄС; впровадження вимог кібербезпеки для продуктів із цифровими елементами; посилення потужностей ЄС з метою виявлення, підготовки й реагування на загрози й інциденти кібербезпеки. Відповідно до Регламенту 2019/881 та Директиви NIS 2 закладено уніфікований підхід щодо забезпечення кібербезпеки у межах ЄС. Обов'язком кожної держави-члена ЄС є розробка і прийняття національних стратегій кібербезпеки, призначення принаймні одного компетентного органу у сфері кібербезпеки, створення національних груп реагування на інциденти комп'ютерної безпеки (CSIRT), призначення єдиного контактного пункту для транскордонного співробітництва, які співпрацюватимуть з Командою реагування на комп'ютерні надзвичайні ситуації для інституцій, органів і агентств ЄС (CERT-EU) та іншими інституціями ЄС у сфері кібербезпеки.

Оптимізація структур, які відповідають за кібербезпеку в Ізраїлі, зумовлена масштабами кіберзагроз в умовах протиборства з арабськими державами. INCD тісно співпрацює з приватним сектором, як безпосередньо, так

і через галузеві центри, що працюють під його егідою. INCD розвиває співпрацю на глобальному та місцевому рівнях, підтримуючи інновації та використовуючи їх. Окрема увага приділяється питанням удосконалення багаторівневої системи підготовки професійних кадрів для сфери кібербезпеки.

Частота і серйозність кібератак з боку Північної Кореї спонукали уряд Південної Кореї оновити Національну стратегію кібербезпеки, яка передбачає зміцнення партнерства з іноземними компаніями і розширення інвестиційних можливостей у поєднанні з внутрішньою індустрією кібербезпеки. Національна служба розвідки (NIS) уповноважена координувати державну політику і здійснювати управління у сфері кібербезпеки. Забезпечення функціонування національної системи кібербезпеки здійснюють колегіальні органи – Рада з питань стратегії національної кібербезпеки і Національна рада з питань протидії кіберзагрозам.

США є одним із світових лідерів розробки стандартів та рекомендацій забезпечення кібербезпеки. Основна дослідницька і наукова місія у питанні кібербезпеки покладена на NIST, який розробляє відповідні стандарти, рекомендації, пропонує кращі практики тощо. Оскільки відсоток приватного сектору у володінні та управлінні критичною інфраструктурою США є значним, тому широко застосовується державно-приватне партнерство у сфері кібербезпеки. Стратегічний план кібербезпеки на 2024-2026 фінансові роки спрямовує зусилля CISA на досягнення нового бачення кібербезпеки, заснованого, зокрема на співпраці з приватним сектором, шляхом запровадження програм обміну інформацією, державних і місцевих грантових програм з метою підвищення безпеки та стійкості приватних компаній у протидії кібератакам.

На нашу думку, ключовим завданням удосконалення національної системи кібербезпеки України є посилення законодавчих засад у цій сфері. У цьому контексті варто зазначити, що Закон України «Про основні засади забезпечення кібербезпеки України» прийнято ще у 2017 році (одинадцять разів внесені зміни, однак вони не є концептуальними і не мають євроінтеграційного спрямування).

Відповідно до Стратегії кібербезпеки України «ключову об'єднувальну та координаційну роль» у національній системі кібербезпеки відіграє Національний координаційний центр кібербезпеки. На прикладі окремих держав-членів ЄС (Латвія, Польща, Угорщина), а також США можна констатувати, що структура і функції органів стратегічного та оперативного управління національними системами кібербезпеки визначено законом. В Україні ж Національний координаційний центр кібербезпеки здійснює свої повноваження відповідно до Положення[65], затвердженого Указом Президента України (зміни останній раз внесені 15 липня 2021 року).

Також у контексті євроінтеграційного шляху України важливим кроком є імплементація актів ЄС у сфері кіберзахисту, насамперед положень Регламенту 2019/881 і Директиви NIS 2. Це стосується законодавчих засад утворення та діяльності національних груп реагування на інциденти комп'ютерної безпеки (CSIRT) і призначення єдиного контактного пункту для транскордонного

[65] Про Національний координаційний центр кібербезпеки : Указ Президента України від 7 червня 2016 року № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text

співробітництва, які співпрацюватимуть з Командою реагування на комп'ютерні надзвичайні ситуації для інституцій, органів і агентств ЄС (CERT-EU) та іншими інституціями ЄС у цій сфері. Варто зазначити, що в Україні функціонують команди реагування державної форми власності, однак забезпечення їх діяльності здійснюється на підзаконному рівні[66]. До прикладу, CSIRT Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації (позаштатна структура), яка функціонує в складі Державної служби спеціального зв'язку та захисту інформації України[67].

У Верховні Раді України зареєстровано проект Закону «Про внесення змін до деяких законів України щодо удосконалення процедур нагляду за кібербезпекою та запровадженням європейських схем сертифікації кібербезпеки»[68], яким пропонується імплементація положень Регламенту 2019/881 та Директиви NIS 2, а також визначення повноважень Національного координаційного центру кібербезпеки (стаття 5^3 проекту). Законопроектом також пропонується визначити: Національну стратегію кібербезпеки документом довгострокового планування; коло суб'єктів забезпечення вимог з кібербезпеки, порядок їх ідентифікації, реєстрації у Реєстрі суб'єктів забезпечення вимог з кібербезпеки; єдиний контактний пункт (стаття 5^2 проекту), що створюється у кожній державі-члені ЄС для забезпечення реалізації інформаційного обміну між основними суб'єктами забезпечення кібербезпеки та координації співробітництва у сфері кібербезпеки; заходи впливу та реагування, які застосовуються до суб'єкта виконання вимог з кібербезпеки за порушення законодавства у сфері кібербезпеки, зокрема встановлення штрафів за невиконання вимог з кібербезпеки.

Зазначена законодавча ініціатива, на нашу думку, є актуальною. Водночас варто врахувати, що високий ступінь ефективності діяльності суб'єктів національної системи кібербезпеки може бути досягнуто винятково за умови створення для них уніфікованих правових рамок і чіткого алгоритму дій. Тому, у контексті удосконалення механізмів державного управління інформаційною безпекою в умовах кіберзагроз, доцільним є створення структури для проведення наукових досліджень і дослідно-конструкторських розробок, а також розширення державно-приватного партнерства (досвід США).

Дослідницька служба
Верховної Ради України

[66] Положення про організаційно-технічну модель кіберзахисту : Затверджено Постановою Кабінету Міністрів України від 29 грудня 2021 року № 1426. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text
[67] Про CSIRT. URL: https://csirt.csi.cip.gov.ua/uk/pages/about-csirt#:~
[68] Про внесення змін до деяких законів України щодо удосконалення процедур нагляду за кібербезпекою та запровадженням європейських схем сертифікації кібербезпеки : Проект Закону від 14.11.2024 № 12207. *Картка законопроекту*. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/45219

Додаток 1

Визначення термінів

№ п\п	Держава	Визначення
1	Україна 	Національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури. Основними суб'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 (частини перша, друга статті 8 Закону України «Про основні засади забезпечення кібербезпеки України»)
2	ЄС 	Екосистема політики кібербезпеки ЄС – мережа безпеки у кіберпросторі, яка включає компетентні інституції ЄС, уніфіковані правила для всіх держав-членів. Реалізуються Агентством ЄС з кібербезпеки (ENISA), яке здійснює свою діяльність на підставі положень Регламенту ЄС 2019/881 Європейського Парламенту і Ради від 17 квітня 2019 року «Про Агентство Європейського Союзу з кібербезпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, а також скасування Регламенту (ЄС) № 526/2013» з іншими спеціальними інституціями
3	Латвія 	Національна політика кібербезпеки полягає у створенні безпечного, відкритого, вільного та надійного кіберпростору, в якому гарантується безпечне, надійне та безперервне отримання та надання послуг, важливих для держави та суспільства, повага до прав людини як у фізичному, так і у віртуальному середовищі. У реалізації політики кібербезпеки визначено пріоритети: захист, стримування та розвиток. Реалізується Національним центром кібербезпеки, функції якого виконує Міністерство оборони у співпраці з іншими суб'єктами у сфері забезпечення кібербезпеки (Стратегія кібербезпеки на 2023-2026 роки, Закон про національну кібербезпеку)
4	Польща 	Національна система кібербезпеки (KSC) – комплексна екосистема співпраці, обміну інформацією та координації діяльності між ключовими суб'єктами, відповідальними за кібербезпеку. Завдання KSC – забезпечення безперебійної роботи ключових сервісів і досягнення високого рівня безпеки ІКТ-систем, від яких залежить ефективна робота держави (статті 3-4 Закону про систему національної кібербезпеки від 5 липня 2018 року)

5	Румунія 	Національна система кібербезпеки (SNSC) розуміється як загальна структура, яка об'єднує для співпраці відповідні органи влади і державні установи, з метою координації дій на національному рівні для забезпечення кібербезпеки. Діяльність SNSC на стратегічному рівні координується Вищою радою національної оборони (CSAT). На оперативному рівні – COSC. Служба розвідки Румунії (SRI) забезпечує технічний секретаріат COSC (статті 6, 7 Закону № 58 від 14 березня 2023 року про безпеку та кіберзахист Румунії та про внесення змін та доповнень до деяких нормативних актів)
6	Ізраїль 	Національну систему кібербезпеки утворюють органи, які здійснюють свою діяльність відповідно до Закону про регулювання безпеки в державних органах від 1998 року, а також підприємства, які розробляють або виробляють обладнання для кібербезпеки (Рішення Уряду № 3611 від 7 серпня 2011 року щодо розвитку національного потенціалу в кіберпросторі). Ізраїльський національний кібердиректорат (INCD) координує діяльність у сфері кіберзахисту та є відповідальним за всі аспекти кіберзахисту (від розробки державної політики та нарощування технологічних потужностей до оперативної діяльності спеціальних підрозділів)
7	Південна Корея 	Термін «національна система кібербезпеки» не має нормативно-правового визначення. Національна система кібербезпеки – сукупність дій повноважних органів у цій сфері. Управління національної безпеки (NSO) є стратегічним координуючим органом. Національна служба розвідки (NIS) уповноважена здійснювати координацію управління у сфері кібербезпеки на оперативному рівні, за погодженням з керівниками відповідних центральних органів влади (Закон про Національну розвідувальну службу №17646 від 15 грудня 2020 року, Указ Президента про правила управління кібербезпекою № 316 від 2 вересня 2013 року зі змінами)
8	США 	Національна система захисту кібербезпеки (NCPS) – інтегрована система, за допомогою якої виявляють випадки вторгнення у кіберпростір, здійснюють аналітику та обмін інформацією тощо і є технологічною основою Агентства з кібербезпеки та безпеки інфраструктури (CISA) для захисту інфраструктури від кіберзагроз (§ 652 розділу 6 Кодексу США)