ПУБЛІЧНЕ УПРАВЛІННЯ У СФЕРІ ДЕРЖАВНОЇ БЕЗПЕКИ ТА ОХОРОНИ ГРОМАДСЬКОГО ПОРЯДКУ

УДК 329.09.5
DOI https://doi.org/10.32782/TNU-2663-6468/2024.1/32

Лисецький Ю.М.
Воєнна академія імені Євгенія Березняка

Старовойтенко О.О.
Інститут соціальної та політичної психології Національної академії педагогічних наук України

Семенюк Ю.В.
Національний університет оборони України

ФОРМУВАННЯ МЕХАНІЗМУ МІЖНАРОДНОЇ КІБЕРБЕЗПЕКИ

У статті доведено, що все більше країн робитимуть ставку на мілітаризацію інформаційного простору й розвиток технологій його безпеки і Україна також надає великого значення своїй міжнародній співпраці у галузі кібербезпеки, активно залучаючись до різних міжнародних колективних зусиль, що сприяють зміцненню кібербезпеки як на національному, так і на міжнародному рівнях. Досліджено формування механізму міжнародної кібербезпеки, як складного і динамічного процесу, який вимагає співпраці держав, міжнародних організацій, індустрії та експертного співтовариства, оскільки кіберзагрози постійно зростають у масштабі та складності. Наведені основні складові такого механізму: міжнародні організації, міжнародні стандарти та норми, міжнародна співпраця та двосторонні угоди, сертифікація та валідація продуктів, кібердетеренція, розробка кіберстратегій. Розглянуті міжнародні організації, які відіграють ключову роль у формуванні та сприянні механізму міжнародної кібербезпеки: International Telecommunication Union, International Organization for Standardization, United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, European Union Agency for Cybersecurity, North Atlantic Treaty Organization, Organisation for Economic Co-operation and Development. Ці організації взаємодіють і співпрацюють, щоб формувати міжнародні стандарти, рекомендації та стратегії у галузі кібербезпеки та забезпечити безпеку в цьому цифровому середовищі. Визначені міжнародні стандарти та норми в галузі кібербезпеки, які є також важливим елементом формування механізму міжнародної кібербезпеки: ISO/IEC 27001 та ISO/IEC 27002, Норми ITU-T X.509, Стандарт IEEE 802.1X, NIST Cybersecurity Framework, EU General Data Protection Regulation. З'ясовано, що успіх формування дієвого механізму міжнародної кібербезпеки визначається ступенем політичної довіри між урядами держав з урахуванням принципів взаєморозуміння, рівноправності і узгодженості інтересів. А забезпечення міжнародної безпеки в світовому кіберпросторі вимагає не тільки зусиль окремих країн світу, а й розробку і здійснення максимально ефективних міжнародних інструментів.

Ключові слова: *кібербезпека, механізм, міжнародні організації, стандарти, норми, сертифікація, валідація, кібердетеренція, кіберстратегія.*

Постановка проблеми. В сучасних умовах все більше країн робитимуть ставку на мілітаризацію інформаційного простору й розвиток технологій його безпеки. Нинішній рівень інформатизації України у цілому й органів державної влади зокрема, нажаль не забезпечує надійного захисту від загроз використання проти української держави кібернаступальних технологій [1]. Тому Україна надає великого значення своїй міжнародній співпраці у галузі кібербезпеки, активно залучаючись до різних міжнародних колективних зусиль, що сприяють зміцненню кібербезпеки як на національному, так і на міжнародному рівнях, а питання фор-

мування механізму міжнародної кібербезпеки є дуже актуальним.

Аналіз останніх досліджень і публікацій. Стан кібербезпеки в Україні і її зв'язок з міжнародною кібербезпекою аналізували Трофіменко О.Г., Прокоп Ю.В., Логінова Н.І., Задерейко О.В. [2]. Кібербезпеку як напрям євроатлантичної інтеграції України розглянув А. Войціховський [3]. Окремі питання формування механізму міжнародної інформаційної безпеки висвітлили Г.А. Піскорська и Н.Л. Яковенко [4]. Разом з тим, проблема формування механізму міжнародної кібербезпеки потрібує більш системних досліджень.

Постановка завдання. Метою статті є дослідження ключових аспектів формування механізму міжнародної кібербезпеки.

Виклад основного матеріалу. Формування механізму міжнародної кібербезпеки є складним і динамічним процесом, який вимагає співпраці держав, міжнародних організацій, індустрії та експертного співтовариства, оскільки кіберзагрози постійно зростають у масштабі та складності. Основними складовими такого механізму є: міжнародні організації, міжнародні стандарти та норми, міжнародна співпраця та двосторонні угоди, сертифікація та валідація продуктів, кібердетеренція, розробка кіберстратегій (рис. 1).

Існує кілька міжнародних організацій, які відіграють ключову роль у формуванні та сприянні механізму міжнародної кібербезпеки.

International Telecommunication Union (ITU) є спеціалізованою агентурою ООН і зосереджується на технічних аспектах телекомунікацій. Вони ведуть роботу над розробкою стандартів та рекомендацій у сфері кібербезпеки, а також сприяють міжнародній співпраці у цьому питанні.

International Organization for Standardization (ISO) встановлює стандарти для різних галузей, включаючи інформаційну безпеку. Стандарти, такі як ISO/IEC 27001, надають рамки для управління кібербезпекою в організаціях незалежно від їхнього місця знаходження.

United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) – група з експертів ООН з питань інформаційної безпеки розробляє звіти та рекомендації щодо поведінки держав в кіберпросторі. Їхні рекомендації сприяють розвитку норм та правил для кібербезпеки.

European Union Agency for Cybersecurity (ENISA) є агентурою Європейського Союзу, яка сприяє підвищенню рівня кібербезпеки в ЄС. Вони розробляють рекомендації, допомагають у виявленні та вирішенні кіберзагроз, та забезпечують координацію на міжнародному рівні.

North Atlantic Treaty Organization (NATO) – визнає кіберпростір як один із основних об'єктів для захисту. Альянс розробляє політику та стратегії кібербезпеки та проводить навчання та вправи для своїх членів.

Organisation for Economic Co-operation and Development (OECD) – сприяє розвитку рекомендацій та настанов щодо кібербезпеки, зокрема стосовно захисту критичної інфраструктури та обміну інформацією між країнами.

Отже, ці організації взаємодіють та співпрацюють, щоб формувати міжнародні стандарти, рекомендації та стратегії у галузі кібербезпеки та забезпечити безпеку в цьому цифровому середовищі.

Міжнародні стандарти та норми в галузі кібербезпеки є важливим елементом формування механізму міжнародної кібербезпеки. Основні стандарти та норми, які визначають цю область:

ISO/IEC 27001 та ISO/IEC 27002 – перший встановлює вимоги до системи управління інформаційною безпекою, а другий надає конкретні рекомендації та практики з імплементації цих вимог. Обидва стандарти визначають основні принципи кібербезпеки, такі як захист інформації та управління ризиками.

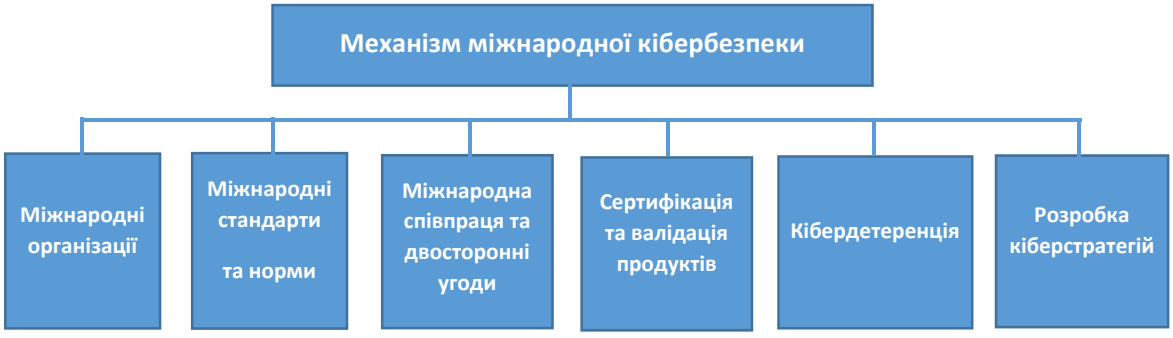

Рис. 1. Основні складові механізму міжнародної кібербезпеки

Норми ITU-T X.509 – визначають формати сертифікатів для захисту ключів та інших даних в системах криптографічного захисту. Вони грають ключову роль у впровадженні публічного ключа та обміні інформацією безпеки.

Стандарт IEEE 802.1X – визначає механізми аутентифікації в бездротових мережах та інших елементах мережевої інфраструктури. Цей стандарт сприяє захисту від несанкціонованого доступу до мережевих ресурсів.

NIST Cybersecurity Framework – визначає базові принципи кібербезпеки та надає рекомендації щодо захисту критичних інфраструктур. Він визначає кібербезпечні функції, такі як захист, виявлення, відповідь та відновлення.

Поведінка держав в інтернеті – група урядових експертів (GGE) ООН з питань інформаційної безпеки визначає норми та правила поведінки держав в кіберпросторі. Їхні звіти визначають, як держави повинні вести себе в мережі, в тому числі під час кіберконфліктів.

EU General Data Protection Regulation (GDPR) – встановлює стандарти для захисту особистих даних громадян Європейського Союзу. Він регулює обробку та передачу цих даних, визначаючи високі стандарти кібербезпеки для компаній, які працюють з особистими даними.

Гармонізовані норми ЄС для кіберзахисту критичних інфраструктур – Європейська комісія розробляє гармонізовані норми для забезпечення кіберзахисту критичних інфраструктур, які визначають вимоги та заходи для захисту ключових секторів від кіберзагроз.

Отже, ці стандарти та норми також визначають рамки та керуючі принципи для розвитку та впровадження стратегій кібербезпеки як на національному, так і на міжнародному рівнях.

Міжнародна співпраця та двосторонні угоди в галузі кібербезпеки є дуже важливими для забезпечення безпеки в цифровому середовищі. До них відносяться:

Інформаційний обмін – держави можуть укладати угоди про обмін інформацією щодо кіберзагроз, виявлення нових загроз та методів атак. Це може включати обмін інформацією про сигнатури загроз, аномалії у виявленні та реагуванні на інциденти.

Забезпечення правопорядку – країни можуть укладати угоди про екстрадицію та правову допомогу у справах кіберзлочинності. Це допомагає у притягненні до відповідальності осіб, які вчиняють кіберзлочини, та сприяє покаранню винних.

Спільні навчальні програми – країни можуть розвивати спільні навчальні та тренувальні програми для підготовки кадрів у сфері кібербезпеки. Це дозволяє підвищувати кваліфікацію фахівців та забезпечувати високий рівень експертизи в області кіберзахисту.

Експертні робочі групи – держави можуть створювати спільні експертні групи для вивчення та аналізу конкретних кіберзагроз. Ці групи можуть визначати кращі практики, обмінюватися дослідженнями та спільно розробляти стратегії відповіді.

Міжнародні конференції та участь у форумах – країни можуть активно брати участь у міжнародних конференціях та форумах з кібербезпеки. Такі заходи дозволяють обмінюватися поглядами на глобальні проблеми та вирішувати їх спільно.

Забезпечення стабільності кіберпростору – двосторонні угоди можуть передбачати зобов'язання щодо запобігання атак на критичну інфраструктуру та забезпечення стабільності кіберпростору.

Спільні ініціативи з розробки технічних стандартів – країни можуть спільно працювати над створенням та розробкою технічних стандартів у галузі кібербезпеки, щоб забезпечити взаємну сумісність та ефективність заходів з захисту.

Отже, двостороння та багатостороння співпраця грає ключову роль у забезпеченні стабільності та безпеки кіберпростору на міжнародному рівні.

Сертифікація та валідація продуктів у сфері кібербезпеки забезпечує високий рівень безпеки та взаємної сумісності в міжнародному кіберпросторі. Міжнародні організації, такі як Міжнародна організація зі стандартизації (ISO) та Інтернаціональна електротехнічна комісія (IEC), розробляють стандарти для кібербезпеки. Продукти, що відповідають цим стандартам, можуть отримати сертифікати відповідності.

Common Criteria (ISO/IEC 15408) – є міжнародним стандартом для оцінки безпеки IT-продуктів. Виробники можуть пройти процес сертифікації, щоб довести, що їхні продукти відповідають визначеним безпечним стандартам.

Federal Information Processing Standards (FIPS) – це федеральні стандарти обробки інформації у Сполучених Штатах Америки, які визначають критерії безпеки для федеральних систем інформаційної обробки. Продукти, які відповідають FIPS, можуть бути використані в урядових системах.

Продукти в різних сферах, таких як мережеві пристрої, антивіруси, криптографічне програмне забезпечення, можуть проходити сертифікацію

для визначених стандартів. Наприклад, криптографічні алгоритми можуть бути сертифіковані Національним інститутом стандартів та технологій (NIST) у США.

Деякі специфічни галузі, такі як медицина, фінанси чи енергетика, можуть мати власні вимоги щодо кібербезпеки. Продукти, що використовуються в цих галузях, повинні проходити валідацію відповідно до специфічних вимог.

Важливу роль відіграє міжнародний обмін сертифікованими продуктами, коли продукт отримує сертифікат відповідності міжнародним стандартам, це полегшує його використання в різних країнах та організаціях, сприяючи гармонізації підходів до кібербезпеки.

Отже, сертифікація та валідація сприяють розвитку та забезпеченню високих стандартів кібербезпеки на міжнародному рівні.

Кібердетеренція – це комплекс заходів та стратегій, спрямованих на виявлення, відслідковування і відповідь на кібератаки, які важливі для формування механізму міжнародної кібербезпеки. До них відносятся наступні:

• виявлення інцидентів – це такі механізми, як системи моніторингу безпеки та інтелектуальні системи аналізу, які допомагають виявляти аномалії та потенційні загрози у реальному часі;

• кіберрозвідка – збір інформації про кіберзагрози, їхні характеристики та методи використання, що дозволяє визначити можливі джерела атак та розробляти стратегії протидії;

• атака змішаних тактик – розробка та використання заходів кібердетеренції, що поєднують технічні, правові та організаційні аспекти, спрямовані на підвищення стійкості та варіативності оборони;

• міжнародний обмін інформацією – створення механізмів для міжнародного обміну інформацією про кіберзагрози та інциденти, який дозволяє ефективніше реагувати та спільно боротися з кіберзлочинністю;

• симуляції та тренування – проведення симуляцій кібератак та тренувань для кіберзахисників, що сприяє розвитку навичок та удосконаленню стратегій оборони;

• співпраця та координація – встановлення міжнародних механізмів співпраці між кіберзахисними агентствами, правоохоронними органами та приватним сектором для обміну інформацією та координації дій;

• юридичні заходи – розробка міжнародних юридичних норм та угод, які визначають правила та відповідальність у кіберпросторі;

• кібердипломатія – використання кібердипломатії для вирішення кіберконфліктів та встановлення міжнародних стандартів у кібербезпеці.

Всі ці заходи утворюють комплексний механізм, спрямований на підвищення стійкості, виявлення та відповідь на кіберзагрози на міжнародному рівні.

Розробка кіберстратегій є ключовою складовою формування механізму міжнародної кібербезпеки. Вона містить:

• визначення загальних принципів (країни можуть розробляти свої кіберстратегії, визначаючи загальні принципи та цілі, спрямовані на підвищення кібербезпеки, наприклад, забезпечення недопущення кібератак на критичну інфраструктуру);

• створення інституційних механізмів (країни можуть встановлювати інституції та агентства, які відповідають за реалізацію та виконання стратегій, наприклад, створення національних центрів кіберзахисту);

• міжнародна співпраця (кіберстратегії часто передбачають міжнародну співпрацю, наприклад, взаємодія з іншими країнами для обміну інформацією про кіберзагрози та спільного реагування на інциденти);

• норми та правила поведінки (розробка кіберстратегій може сприяти формулюванню міжнародних норм та правил поведінки в кіберпросторі, наприклад, визначення правил відповідальності за кібератаки);

• захист критичної ынфраструктури (країни можуть включати стратегії забезпечення захисту критичної інфраструктури від кіберзагроз для таких секторів, як енергетика, транспорт, телекомунікації та інші);

• боротьба з кіберзлочинністю (кіберстратегії можуть передбачати заходи для боротьби з кіберзлочинністю та кібершахрайством як на національному, так і на міжнародному рівні);

• розробка технічних засобів (країни можуть включати в свої кіберстратегії розробку технічних рішень та інновацій для захисту від кіберзагроз);

• участь у міжнародних організаціях (країни можуть приєднуватися до міжнародних організацій, таких як Інтерпол чи ООН, для спільних зусиль у сфері міжнародної кібербезпеки);

Отже, розробка та реалізація кіберстратегій дозволяють країнам ефективно управляти та реагувати на загрози в кіберпросторі, сприяючи формуванню загальносвітового механізму міжнародної кібербезпеки.

Висновки. Успіх формування дієвого механізму міжнародної кібербезпеки визначається ступенем політичної довіри між урядами держав з урахуванням принципів взаєморозуміння, рівноправності і узгодженості інтересів. А забезпечення міжнародної безпеки в світовому кіберпросторі вимагає не тільки зусиль окремих країн світу, а й розробку і здійснення максимально ефективних міжнародних інструментів.

Список літератури:

1. А.О. Худолій. Acta de Historia & Politica: Saeculum XXI. 2020. С. 138–146.

2. Трофіменко О. Г., Прокоп Ю.В., Логінова Н.І., Задерейко О.В. Кібербезпека України: аналіз сучасного стану. Захист інформації. Том 21. 2019, № 3. С. 150–157.

3. Войціховський А. В. Кібербезпека як напрям євроатлантичної інтеграції України. Право і безпека у контексті європейської та євроатлантичної інтеграції: збірник статей та тез наукових повідомлень за матеріалами дискусійної панелі II Харківського міжнародного юридичного форуму, м. Харків, 28 вересня 2018 р. / редкол: Ю. Г. Барабаш, Т. М. Анакіна, Д. В. Аббакумова. Харків : Право, 2018. С. 42–48.

4. Піскорська Г.А., Яковенко Н.Л. Сучасні виклики і загрози в кіберпросторі: формування механізму міжнародної інформаційної безпеки. Міжнародні відносити, 2018. № 18-19 (2). URL: https://cutt.ly/GQCBYfV (дата звернення 16.12.2023).

Lysetsyi Yu.M., Starovoytenko O.O., Semenyuk Yu.V. FORMATION OF THE MECHANISM OF INTERNATIONAL CYBERSECURITY

The article explains how more and more countries will focus on the militarization of the information space and the development of its security technologies in close future. It is emphasized in the article, that Ukraine also attaches great importance to its international cooperation in the field of cybersecurity, actively participating in various international collective efforts that contribute to the strengthening of cybersecurity at both the national and international levels. The article shows that formation of an international cybersecurity mechanism is a complex and dynamic process that requires the cooperation of states, international organizations, industry, and the expert community, as cyber threats are constantly growing in scale and complexity. The article presents the main components of such a mechanism that include international organizations, international standards and norms, international cooperation and bilateral agreements, product certification and validation, cyber deterrence, and the development of cyber strategies. Different international organizations that play a key role in the formation and promotion of the international cybersecurity mechanism include the International Telecommunication Union, International Organization for Standardization, United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, European Union Agency for Cybersecurity, North Atlantic Treaty Organization, Organization for Economic Co-operation and Development are presented in the article. These organizations interact and cooperate to develop international standards, recommendations, and strategies in the field of cybersecurity and to ensure safety in this digital environment. The article also presents international standards and norms in the field of cybersecurity as an important element in the formation of the international cybersecurity mechanism. The main standards and norms in the field of cybersecurity include: ISO/IEC 27001 and ISO/IEC 27002, ITU-T X.509 standards, IEEE 802.1X standard, NIST Cybersecurity Framework, EU General Data Protection Regulation. The article proves, that success of forming an effective international cybersecurity mechanism is determined by the degree of political trust between the governments of states, taking into account the principles of mutual understanding, equality, and the alignment of interests. Ensuring international security in the global cyberspace requires not only the efforts of individual countries of the world but also the development and implementation of the most effective international tools.

Key words: *cybersecurity, mechanism, international organizations, standards, norms, certification, validation, cyber deterrence, cyber strategy.*