МІЖНАРОДНО-ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В РАМКАХ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ

КАВИН Святослав Ярославович - аспірант, кафедра європейського права, факультет міжнародних відносин Львівський національний університет імені Івана Франка

ORCID: 0000-0002-6189-3848
DOI 10.32782/EP.2023.2.24

Стаття присвячена аналізу та вивченню правових механізмів міжнародних організацій у сфері забезпечення інформаційної безпеки. Правові акти щодо міжнародної інформаційної безпеки, які приймаються у форматі міжнародних організацій, зокрема ITU; IEEE; ISO, виступають керівними принципами діяльності багатосторонніх міжнародних відносин з врахуванням позицій та інтересів усіх міжнародних учасників. Відповідно комплексне дослідження загальних закономірностей функціонування та розвитку міжнародно-правових механізмів забезпечення інформаційної безпеки в рамках діяльності міжнародних організацій є особливо доречним, актуальним і потребує детального аналізу.

Ключові слова: міжнародна інформаційна безпека, міжнародне право, міжнародні організації, міжнародно-правові акти, стандарти, правові механізми.

Вступ

Формування багатовекторного середовища правового забезпечення захисту інформації, вимагає системного підходу і відповідно здійснення аналізу правових оцінок ризиків інформаційної безпеки враховуючи особливості інформаційних правовідносин в сучасних умовах глобальної інформатизації суспільства. Тому, в цьому плані, особливо актуальним є вироблення дієвих механізмів забезпечення міжнародної інформаційної безпеки зокрема завдяки діяльності міжнародних організацій. В цьому контексті, на передній план виходить формування правових механізмів, які спрямовані на забезпечення та дотримання безпеки інформаційного простору.

Відповідно дослідження впливу міжнародних організацій на формування правового поля забезпечення інформаційної безпеки і як регулятора дій в області міжнародних інформаційних правовідносин, знаходиться в юрисдикції актуальних міжнародних проблем, для вирішення яких необхідною є успішна діяльність та взаємодія всіх учасників міжнародних відносин. У зв'язку з цим проблематика становлення якісно нової системи міжнародної інформаційної безпеки є важливою та актуальною, і процес регулювання з боку міжнародних організацій відіграє значну роль в трансформації світової системи міжнародної безпеки.

Мета дослідження

Дослідження загальних закономірностей функціонування та розвитку міжнародно-правових механізмів забезпечення інформаційної безпеки в рамках діяльності міжнародних організацій та розробка науково-обґрунтованих пропозицій і рекомендацій стосовно ефективної дії даних механізмів в міжнародному та національних правопорядках.

Аналіз досліджень і публікацій

Вагомий внесок у дослідження впливу міжнародних організацій в сфері інформаційної безпеки зробили такі відомі вітчизня-

ні науковці, як А.П. Голіков, М.В. Гуцалюк, Жовтий, І.М., Захаренко К., Забара, Л.І. Капінус, В.О. Козуб, Б.А. Кормич, В.А. Ліпкан, О.В. Логінов, Ю.Є. Максименко, А.І. Марущак, Вонсович О.С. зокрема міжнародний досвід забезпечення інформаційної безпеки як складової системи національної безпеки, а також правові засади інформаційної безпеки та питання її правового регулювання в рамках міжнародних організацій висвітлювали у своїх роботах Кононенко В.П. [6], Новікова Л.В., [6] Алексєєва Т. І., [3] Копійка М.В., [7] Нашинець-Наумова А.Ю., [10] Войціховський А.В., [5] Макаренко Є. А., [9] Рижиков М. М., [9] Ожеван М. А., [9] Головченко В. І., [9] Гондюл В. П., [9] Фролова О.М., [11] Шемчук В.В. [12] та інші. В своїх дослідженнях особлива увага приділялась аналізу правової діяльності міжнародних інституцій в контексті характеристики міжнародних правових механізмів протидії новим викликам для системи міжнародної безпеки.

Серед зарубіжних учених проблемою діяльності міжнародних організацій у сфері інформаційної безпеки займалися: Зб. Бжезинський, М. Дженіс, Б. Гейтс, Е. Бредлі, Г. Анхейер, К. Хагаі, З. Тофлер, У. Шрамм, Результати досліджень щодо правового регулювання діяльності міжнародних організацій в сфері інформаційної безпеки висвітлювали в своїх роботах, Cebrovski A., [26] Garstka J., [26] Duncan B. Hollis, [27] Matthew C. Waxman, [27] Kubo Mačák, [31] Libicki M.C., [32] Mazur, M., [33] Robinson, N., [36] Gaspers, J. [36] та інші. Акцент в роботах був сконцентрований на аналізі правового інструментарію інформаційних та кіберзагроз для системи міжнародної безпеки, особлива увага була приділена міжнародному нормативно-правовому співробітництву щодо інформаційної безпеки на рівні міжнародних організацій.

Але незважаючи на широкий спектр наукових досліджень у сфері інформаційної безпеки, в сучасній науці не приділялася достатня увага детальному аналізу правового регулювання діяльності міжнародних організацій у цій сфері. В цьому контексті, очевидною є актуальність дослідження в рамках міжнародного права, впливу діяльності міжнародних організацій на забезпечення інформаційної безпеки.

Виклад основного матеріалу

Основними найбільшими та відомими міжнародними професійними об'єднаннями, так чи інакше пов'язаними з питаннями інформаційної безпеки, є: Міжнародна спілка електрозв'язку /International Telecommunication Union (ITU)/; Інститут інженерів з електротехніки та електроніки /Institute of Electrical and Electronics Engineers (IEEE)/; Асоціація обчислювальних машин/Association for Computing Machinery (ACM)/; Всесвітній веб -консорціум / World Wide Web Consortium (W3Consortium (W3C))/; Асоціація безпеки інформаційних систем /Information Systems Security Association (ISSA)/; Міжнародна організація зі стандартизації /International Organization for Standardization (ISO)/; Інтернет -інженерна група /Internet Engineering Task Force (IETF)/; Міжнародна асоціація комп'ютерної безпеки /International Computer Security Association (ICSA)/; Асоціація аудиту і контролю інформаційних систем / Information Systems Audit and Control Association (ISACA)/; Альянс інтернет-безпеки / Internet Security Alliance (ISA)/.

Тут важливо відмітити, що створення ефективної та надійної системи забезпечення інформаційної безпеки видається надзвичайно важливим в контексті трансформації міжнародної безпеки та зовнішньої політики. В цьому контексті важливого значення набуває трансформація системи міжнародної безпеки на основі адаптації міжнародних стандартів інформаційної безпеки. [37]

Разом з тим, інформатизація суспільства, а відповідно, зростання можливості несанкціонованого вторгнення в мережу та доступу до інформації, сприяло появі нових спеціалізованих міжнародних організацій у сфері інформаційної безпеки. Основним напрямом діяльності таких спеціалізованих міжнародних організацій та об'єднань, є формування та підтримання баз даних, що містять інформацію про відомі вразливості різних програмних та апаратних засобів, а також інші форми та напрямки інформацій-

ної, консультативної та методичної роботи в даній сфері. Сьогодні можна назвати такі найбільш значні організації, як: Координаційний центр комп'ютерної групи реагування на надзвичайні ситуації Інституту інженерії програмного забезпечення /Coordination Center of the Computer Emergency Response Team (CERT Coordination Center (CERT/CC)) for the Software Engineering Institute (SEI)/ та Дослідницька група X-Force компанії IBM.

Вплив міжнародних організацій на формування міжнародної правової системи інформаційної безпеки є важливим фактором у вирішенні проблем стабільності та надійності світового інформаційного простору, а це спонукає до розвитку нових правовідносин в системі тотальної інформатизації суспільства. Як зауважують Лужицький В. А. та Кожухівський А. Д., механізм функціонування інформаційного простору нині став планетарним фактором, породивши цілу низку соціальних трансформацій, ввівши в систему соціальних відносин такі процеси, як інформаційні війни, інформаційна зброя, інформаційний тероризм, інформаційна злочинність та інформаційна безпека [6]. В цьому контексті формування правових механізмів, котрі спрямовані на забезпечення та дотримання безпеки інформаційного простору передбачають вдосконалення та гармонізацію нормативно-правової бази у сфері інформаційної безпеки як на національному так і міжнародному рівнях. А це у свою чергу зумовлює необхідність дослідження комплексу питань котрі пов'язані із забезпеченням та дотриманням контролю над інформаційною інфраструктурою. Що у свою чергу зумовлює необхідність вивчення та узгодження правових механізмів завдяки яким забезпечується захист інформаційної безпеки. [4]

У зв'язку з цим проблематика становлення якісно нової системи міжнародної інформаційної безпеки є дуже актуальною, і процес регулювання з боку міжнародних організацій відіграє значну роль як для економічного так і для соціально-політичного розвитку кожної країни окремо і суспільства загалом.

Міжнародна спілка електрозв'язку - International Telecommunication Union (ITU)

ITU є найстарішою міжнародною організацією, пов'язаною з інформаційними технологіями. В даний час ITU об'єднує 189 держав. Основним її завданням спочатку було управління та координація діяльності у сфері передачі інформації. Однак у міру розвитку глобальних комп'ютерних мереж та інтеграції комп'ютерних і телекомунікаційних систем, область діяльності ITU була значно розширена і в даний час включає безліч питань, пов'язаних з побудовою комп'ютерних мереж, передачею цифрових даних, обробкою інформації і т.п. Проф. Френсіс Лайалл (Francis Lyall), який був учасником правління Європейського центру космічного права та є директором Міжнародного інституту космічного права, а також був учасником групи юридичних експертів INTELSAT та входив до групи реформ ITU, провів сучасний аналіз розвитку ITU від початку до теперішнього часу, в контексті оперативного реагування на законодавчому рівні на технічні та політичні зміни і виокремив пропозиції на майбутній розвиток організації, зокрема формування правового поля забезпечення інформаційної безпеки. [28].

Міжнародний союз електрозв'язку нині є спеціалізованим агентством ООН і займається питаннями в галузі телекомунікацій. Для забезпечення безпечного використання засобів електрозв'язку учасниками Міжнародного союзу електрозв'язку було застосовано стандарт DPI «Глибока перевірка пакетів» для знищення вірусів, які попадали несанкціоновано у комп'ютерну мережу. Застосування новітніх технологій є прикладом прогресу в галузі інформаційних систем і переходом до високих стандартів електрозв'язку. [1], [2] В цьому контексті важливо відмітити, що в документі ITU «Розуміння кіберзлочинності: Явище, завдання та законодавча відповідь», проф. Марко Герке (Prof. Dr. Marco Gercke), розглядає першу із семи стратегічних цілей Глобальної програми кібербезпеки ITU, яка відмічає необхідність ретельної розробки стратегій для створення законодавства щодо боротьби з кіберзлочинністю на гло-

бальному рівні у взаємодії з національними законодавчими актами, а також розглядає підхід щодо організації національних зусиль у боротьбі з кіберзлочинністю, що розробляється 1-ою Дослідницькою комісією ITU-D у рамках Питання 22/1. [34]

Вищим органом влади ITU є Повноважна Конференція ***(Plenipotentiary Conference)*** - збори делегацій держав – учасників ITU, що відбуваються раз на чотири роки. Основні виконавчі органи - Рада та Генеральний секретаріат ITU. Основні робочі підрозділи поділені на три сектори:

- сектор стандартизації зв'язку, ITU-T;
- сектор радіозв'язку, ITU-R;
- сектор розвитку електрозв'язку ITU-D.

ITU-R та ITU-D виконують окремі дослідницькі, координаційні та технічні функції, тоді як Сектор стандартизації зв'язку – ITU-T більшою мірою відповідає за вирішення стратегічних завдань розвитку інформаційних технологій та інфраструктури, зокрема, за розробку методик та стандартів, необхідних для всього світового співтовариства.

Учасниками ITU-T є:

- державні органи влади (міністерства та відомства зв'язку окремих країн);
- наукові організації та компанії – виробники телекомунікаційного обладнання;
- регіональні та міжнародні телекомунікаційні організації.

Функціональними органами ITU-T є:

- Всесвітня асамблея зі стандартизації телекомунікацій ***(World Telecommunication Standardization Assembly)***, що проводиться кожні чотири роки, – основний керівний орган сектору стандартизації;
- Бюро зі стандартизації телекомунікацій ***(Telecommunication Standardization Bureau)*** – виконавчий підрозділ сектору стандартизації;
- Дослідницькі групи (загалом їх 14);
- Консультативна група стандартизації телекомунікацій ***(Telecommunication Standardization Advisory Group)*** – допоміжний підрозділ, який здійснює координаційну роботу.

Основною метою роботи ITU-T є розробка універсальних рекомендацій та міжнародних стандартів, що належать до різних сфер телекомунікаційних технологій та управління телекомунікаціями. З точки зору забезпечення інформаційної безпеки найбільш значущими стали рекомендації щодо серії «X – мережі передачі даних і зв'язок відкритих систем» і, зокрема, до серії «X.8xx – безпека», зокрема можна відмітити:

ITU-T X.1054 (04/2021) [17] Рекомендація ITU-T X.1054 | Міжнародний стандарт ISO/IEC 27014 надає вказівки щодо управління інформаційною безпекою, оскільки, управління інформаційною безпекою забезпечує потужний зв'язок між керівними органами та виконавчими структурами в контексті впровадження та експлуатації системи управління інформаційною безпекою. Разом з тим створюються реальні можливості для формування повноважень, необхідних для впровадження ініціатив у сфері інформаційної безпеки в усій організації. Крім того, ефективне управління інформаційною безпекою гарантує, що керівний орган отримує відповідну звітність – оформлену в бізнес-контексті – про діяльність, пов'язану з інформаційною безпекою. Це дозволяє прийняти відповідні та своєчасні рішення щодо питань інформаційної безпеки на підтримку стратегічних цілей організації.

ITU-T X.1052 (10/2020) [18] Рекомендація ITU-T X.1052 описує та рекомендує структуру управління інформаційною безпекою (ISMF) яка базується на процесному підході для опису набору областей управління безпекою і відповідно надають практичні методології, зосереджені на конкретній області управління інформаційною безпекою.

ITU-T X.1631 (07/2015) [19] Рекомендація ITU-T X.1631 | ISO/IEC 27017 Міжнародний стандарт надає вказівки щодо засобів керування інформаційної безпеки, застосовних до надання та використання хмарних послуг, зокрема додаткові настанови щодо впровадження відповідних засобів контролю, визначених у ISO/IEC 27002, а також додаткові елементи керування з інструкціями щодо впровадження, які стосуються саме хмарних служб.

Питання інформаційної безпеки знайшли своє відображеня також в наступних

Стандартах: ITU-T X.1352 (09/2022); ITU-T X.1814 (09/2022); ITU-T Y.3539 (01/2023)

Відповідно до Резолюції 1 Всесвітньої асамблеї зі стандартизації телекомунікацій 2000-го року, було запроваджено практику призначення Провідних дослідницьких груп ***(Lead Study Groups, LSGs)*** з певних питань, що потребують одночасної координації зусиль кількох дослідницьких груп, що працюють у різних галузях. В цьому контексті, починаючи з вересня 2001 року, функціонує «Дослідна група 17: Мережі передачі даних та телекомунікаційне програмне забезпечення» ***(«Study Group 17: Data Networks and Telecommunication Software»)***, яка була утворена на основі існуючих до цього «Дослідницької групи 7» та «Дослідної групи 10» . Вона є Провідною дослідною групою з питань безпеки комунікаційних систем ***(Communication Systems Security, (CSS))*** і, відповідно, не тільки працює над забезпеченням безпеки інформаційних технологій, що безпосередньо належать до її компетенції, але й займається питаннями безпеки різних комунікаційних технологій, що розробляються іншими дослідницькими групами. Однією з найбільш значущих розробок цієї групи у сфері інформаційної безпеки вважається Стандарт ***X.509***, який заклав основи розвитку інфраструктури громадських ключів. Найбільш актуальними проблемами, над якими нині працює Провідна дослідницька група з питань безпеки комунікаційних систем, є: керування безпекою; безпека мобільних систем; безпека систем зв'язку служб реагування на надзвичайні ситуації.

У цілому робота цієї дослідницької групи охоплює досить широкий діапазон сфер щодо забезпечення безпеки серед яких можна виділити таку як техніка забезпечення безпеки (на сьогодні включає роботу над рекомендацією X.841 – Об'єкти інформаційної безпеки для контролю доступу)

Крім розробки рекомендацій та стандартів, одним із важливих напрямів роботи ITU також стало забезпечення інформаційного обміну, з використанням різних платформ, щодо забезпечення інформаційної безпеки. Одним з найбільш масштабних заходів є Всесвітній саміт з інформаційного суспільства ***(WSIS: The World Summit On The Information Society)***.

Institute of Electrical and Electronics Engineers (IEEE) – Інститут інженерів з електроніки та електротехніки

IEEE є однією з найвідоміших професійних організацій, що існує з 1884 року і в даний час налічує близько 380000 учасників зі 150 країн світу. Основні напрямки роботи цієї організації: проведення спеціалізованих професійних конференцій; публікація спеціалізованих видань; підтримка освітньої діяльності; підтримка інноваційних технічних та методичних розробок у різних сферах; розробка та розповсюдження технічних стандартів. Зокрема IEEE 802 це основний стандарт IEEE для локальних і регіональних мереж, що включає огляд мережної архітектури, який був схвалений ще у 1990 році. Цей стандарт визначає, як уся мережа або її частина може бути прозоро захищена. А з розвитком інформаційного суспільства і відповідно збільшенням ризиків інформаційних загроз, в документ регулярно вносяться додатки для забезпечення необхідної інформаційної безпеки, зокрема:

IEEE/ISO/IEC 8802-1AE-2013 [13] Міжнародний стандарт ISO/IEC/IEEE для інформаційних технологій. Телекомунікації та обмін інформацією між системами. Локальні та міські мережі. Частина 1AE. Безпека керування доступом до середовища (MAC). ***ISO/IEC/IEEE International Standard for Information technology -- Telecommunications and information exchange between systems -- Local and metropolitan area networks -- Part 1AE: Media access control (MAC) security***

IEEE/ISO/IEC 8802.1AR-2014 [14] Міжнародний стандарт ISO/IEC/IEEE для інформаційних технологій. Телекомунікації та обмін інформацією між системами. Локальні та міські мережі. Частина 1AR. Захищена ідентифікація пристрою. ***ISO/IEC/IEEE International Standard for Information technology -- Telecommunications and information exchange between systems -- Local and metropolitan area networks -- Part 1AR: Secure device identity***

IEEE/ISO/IEC 8802-11:2018/Amd 1-2019 [15] Міжнародний стандарт IEEE/ISO/IEC. Інформаційні технології. Телекомуніка-

ції та обмін інформацією між системами. Локальні та міські мережі. Особливі вимоги. ***IEEE/ISO/IEC International Standard - Information technology-Telecommunications and information exchange between systems - Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications***

IEEE 802.11-2020 [16] Стандарт IEEE для інформаційних технологій. Телекомунікації та обмін інформацією між системами. Локальні та міські мережі. Специфічні вимоги. ***IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications***

Науковці Джозеф Р. Геркерт (Joseph R. Herkert) та Крістін С. Нільсен (Christine S. Nielsen), відмічають, що IEEE визначили електронні медіа як стратегічну технологію для комунікації та розповсюдження інформації і визнало дедалі більшу залежність від електронних медіа. В звязку з цим були проведені дослідження для оцінки соціальних, організаційних та економічних наслідків зміни щодо діапазону та глибини впливу, типів переваг та небажаних ефектів. Відповідно, на основі результатів досліджень були надані рекомендації щодо того, як наукові та технічні організації можуть повною мірою скористатися перевагами електронних медіатехнологій, одночасно вживаючи заходів, щоб уникнути негативних наслідків цих технологічних змін. [29]

До складу IEEE входять 10 регіональних відділень, 38 професійних товариств. Поточне управління діяльністю здійснюється Радою директорів та Виконавчим комітетом, роботу яких очолюють Президент та Виконавчий директор.

Одним із основних підрозділів IEEE, що спеціалізуються на питаннях інформаційної безпеки, є Технічний комітет з безпеки та захисту приватної інформації – ***«IEEE Computer Society Technical Committee on Security and Privacy»*** . У його складі функціонують три підкомітети:

• Підкомітет із стандартів ***(Subcommittee on Standards)***;

• Підкомітет з академічної роботи ***(Subcommittee on Academic Affairs)***;

• Підкомітет зі спеціалізованих конференцій ***(Subcommittee on Security Conferences)***.

Основними заходами, які проводить цей комітет, є:

• Щорічний симпозіум з безпеки та захисту приватної інформації ***(IEEE CS Symposium on Security and Privacy)***;

• Щорічний семінар з основ інформаційної безпеки ***(Computer Security Foundations Workshop)***.

Також комітет веде роботу зі збирання та узагальнення актуальної інформації про події у співтоваристві фахівців з інформаційної безпеки. Спеціальний інформаційний бюлетень із цією інформацією – ***«Cipher»*** – розсилається передплатникам у середньому один раз на два місяці.

International Organization for Standardization (ISO) – Міжнародна організація зі стандартизації

ISO у нинішньому вигляді було засновано 1946г. і є неурядове об'єднання національних організацій зі стандартизації, націлене на уніфікацію стандартів (головним чином, технічних) у різних галузях виробничої діяльності та надання послуг.

Крім основних учасників (156 країн), які безпосередньо беруть участь у роботі, в ISO також входять учасники-кореспонденти ***(Correspondent member)*** – країни, які не мають повноцінних органів стандартизації, а також учасниками-підписниками ***(Subscriber member)*** – країни з невеликими економіками, які отримують необхідну довідкову інформацію на пільгових умовах.

Головним органом управління ISO є щорічна Генеральна Асамблея, яка приймає стратегічні рішення щодо розвитку всієї організації. Підготовкою матеріалів для прийняття таких рішень займається Рада ISO, збори якої відбуваються двічі на рік. Безпосередньо розробкою стандартів займаються технічні комітети та підкомітети, у яких беруть участь представники заінтересованих країн. За розробку кожного документа у підкомітеті відповідає спеціально створена для цього робоча група. Проекти міжна-

родних стандартів, прийняті технічними комітетами, надсилаються до національних організацій для голосування; документ набуває статусу міжнародного стандарту, якщо за нього проголосувало не менше 75% учасників, які брали участь у голосуванні.

Основним підрозділом ISO, що займається питаннями інформаційної безпеки, є Об'єднаний технічний комітет JTC 1 «Інформаційні технології», до складу якого входить підкомітет ***SC 27*** «Засоби безпеки в інформаційних технологіях» ***(IT Security techniques)***. За час своєї роботи цей підкомітет розробив понад 60 міжнародних стандартів щодо інформаційної безпеки.

З питаннями інформаційної безпеки також пов'язана робота підкомітету ***SC 37*** «Біометрична ідентифікація» ***(Biometrics)*** та підкомітету ***SC 17*** «Картки та персональна ідентифікація» ***(Cards and personal identification)***.

Стандарти інформаційної безпеки це сімейство стандартів ISO 2700X Індивідуальні стандарти інформаційної безпеки серії ISO 2700x стосуються різноманітних тем у сфері інформаційної безпеки. Наприклад, міжнародний стандарт визначає ISO 27001 – система управління інформаційною безпекою (ISMS), ISO 27701 – систему управління захистом даних, ISO 27017 містить рекомендації щодо заходів інформаційної безпеки для хмарних обчислень, а ISO 27005 – рекомендації щодо управління ризиками інформаційної безпеки. В цьому контексті необхідно відмітити стандарти:

ISO 27001 ***(ISO/IEC 27001:2022 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи управління інформаційною безпекою. Вимоги)*** - Вимоги до систем управління інформаційною безпекою [20] Це міжнародно визнаний стандарт інформаційної безпеки, яка охоплює не тільки аспекти IT-безпеки. Документ надає модель для встановлення, впровадження, моніторингу та підвищення рівня захисту. Мета полягає в тому, щоб визначити потенційні ризики, проаналізувати та зробити їх контрольованими за допомогою відповідних заходів. ISO 27001 формулює вимоги до такої системи управління, які перевіряються як частина зовнішнього процесу сертифікації.

Оптимальною основою для ефективної реалізації цілісної стратегії безпеки є добре структурована система управління інформаційною безпекою (СУІБ) відповідно до стандарту ISO 27001.

ISO 27019 (*ISO/IEC 27019:2017 Інформаційні технології - Методи безпеки - Контроль інформаційної безпеки для енергетичних підприємств)*- Заходи інформаційної безпеки для енергопостачання. [21] Документ формулює додаткові заходи для енергетичного сектора.

ISO 27006 ***(ISO/IEC 27006:2015 Інформаційні технології. Методи безпеки — Вимоги до органів, що здійснюють аудит та сертифікацію систем управління інформаційною безпекою)*** - Вимоги до органів сертифікації [22] ISO 27006 спрямований на такі органи, як DQS, які здійснюють сертифікацію систем управління інформаційною безпекою. Документ описує вимоги, яких органи сертифікації повинні дотримуватися при оцінці систем менеджменту своїх клієнтів відповідно до ISO 27001 для сертифікації.

ISO 27002 ***(ISO/IEC 27002:2022 Інформаційна безпека, кібербезпека та захист конфіденційності — засоби контролю інформаційної безпеки)*** - Керівництво з контролю інформаційної безпеки [23]

ISO 27017 ***(ISO/IEC 27017:2015 Інформаційні технології - Методи безпеки - Кодекс практики контролю інформаційної безпеки на основі ISO/IEC 27002 для хмарних служб)*** – Керівництво із заходів інформаційної безпеки в хмарних сервісах [24] Цей документ надає рекомендації щодо заходів інформаційної безпеки в хмарних обчисленнях у рамках стандартів інформаційної безпеки. Він рекомендує, підтримує та надає додаткові заходи для впровадження спеціальних засобів управління інформаційною безпекою.

ISO 27005 ***(ISO/IEC 27005:2022 Інформаційні технології - Методи захисту IT - Управління ризиками інформаційної безпеки.)*** - Керівництво з управління ризиками інформаційної безпеки. [25] Цей документ надає рекомендації щодо управління ризиками інформаційної безпеки та підтримує

загальні концепції щодо цього, викладені в ISO 27001. ISO 27005 також призначений для підтримки впровадження інформаційної безпеки на основі концепції управління ризиками.

Слід зауважити, що детальний аналіз діяльності організації, зокрема в контексті формування узгодженого правового поля з національними законодавствами на основі єдиних стандартів проводили в своїх дослідженнях проф. (Jonathan Koppell) та проф. (Craig N. Muphy).

Досліджуючи роль Міжнародної організації зі стандартизації (ISO) як координатора (фасилітатора) у створенні необхідної економічної інфраструктури, а також значення методів ISO для значно ширшої сфери глобального управління, Мерфі (Craig N. Muphy) та Єйтс (JoAnne Yates) представили комплексний огляд ISO як потужної сили, що впливає на те, як здійснюються міждержавні звязки. Разом з тим вони відмічають, що хоча ISO не має повноважень змушувати прийняти свої стандарти, тим не менш, тиск щодо впровадження стандартів ISO може бути багатогранним і досить сильним. [35]

Стандарти ISO прийняті у юрисдикціях по всьому світу і часто у міждержавних відносинах наголошується на ринковому аспекті «м'якого права» впровадження стандартів ISO, але не слід забувати про ступінь, в якому стандарти ISO також інтегровані в «жорстке право», як внутрішні, так і міжнародні закони, зауважує Копел (Jonathan Koppell) Навіть ISO, яка чітко вказує, що вона не «регулює і не видає законів», визнає, що «хоча стандарти ISO є добровільними, вони можуть стати ринковими вимогами». Це відображає те значення, яке індустрія надає стандартизації, і той факт, що стандарти часто набувають чинності внутрішнього законодавства через їх включення у внутрішню та міжнародну правову базу. [30]

Висновок

Темпи розвитку сучасних інформаційних технологій значно випереджають темпи розробки рекомендаційної та нормативно-правової бази міжнародних керівних документів в сфері інформаційної безпеки. Відповідно для ефективного і оперативного визначення критеріїв оцінки ефективності захисту інформації (рівня інформаційної безпеки), окрім встановлених вимог, рекомендацій та керівних документів важливим і необхідним елементом є застосування методики міжнародних стандартів (зокрема ISO/IEC, які розроблені спільним технічним комітетом Міжнародної організації з стандартизації (ISO) та Міжнародної електротехнічної комісії (IEC)), що дає можливість максимально забезпечити захист інформації і мінімізувати ризики

інформаційної безпеки у сукупності з оцінками ефективності інвестицій в забезпеченні безпеки і захисту інформації.

Важливими елементами організаційної роботи на рівні міжнародних структур є організація обміну знаннями та актуальними новинами з інформаційної безпеки у різних формах, а також організація і підтримка в актуальному стані відповідних баз даних та баз знань, для правового забезпечення інформаційної безпеки. Але кожна з міжнародних організацій має свої специфічні організаційні особливості, проте всі вони, як правило, вирішують завдання розробки, погодження та подальшого поширення правових та організаційних рішень щодо правил побудови глобальних мереж обміну даними інфраструктури інформаційної безпеки.

В цілому нині діяльність в області інформаційної безпеки на рівні міжнародних структур не є універсальною і вони будують свою роботу самостійно, створюючи свої норми і нормативи. Зважаючи на те, що така форма організаційної роботи заснована на приватних компаніях, підходи до організації та управління зазвичай не підпорядковуються будь-яким загальним правилам. Тобто єдиної нормативно-правової бази для надійного і ефекивного забезпечення інформаційної безпеки поки немає. Відповідно виникає гостра необхідність створення єдиного Стандарту забезпечення інформаційної безпеки для всіх структур та організацій під егідою єдиної міждержавної Інституції в рамках міжнародного права.

Література

1 Конвенція Міжнародного союзу електрозв'язку URL: https://zakon.rada.gov.ua/laws/show/995_100#Text (звернення 10.03.2023)

2 Статут Міжнародного союзу електрозв'язку URL: https://zakon.rada.gov.ua/laws/show/995_099#Text (звернення 10.03.2023)

3 Алексєєва Т. І., Міжнародні організації: сучасні пріоритети та нові виклики в системі міжнародної інформаційної безпеки. Науковий вісник Ужгородського національного університету 2020. № 34 С. 9-12.

4 Кавин С., Брацук І. Нормативно-правові механізми забезпечення кібербезпеки в нових державах – членах ЄС // Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки. – 2021 - № 2 (117) – С.30-38

5 Войціховський А.В. нформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). Вісник Харківського національного університету імені В.Н.Каразіна. Серія «ПРАВО». 2020. № 29. С. 281-288.

6 Кононенко В.П., Новікова Л.В., Копицька П.О. Політика міжнародних організацій з питань інформаційної безпеки Науковий вісник Ужгородського національного університету, серія право 2021. № 65 С. 353-358.

7 Копійка М.В. Модернізація політики міжнародних організацій у сфері інформаційної безпеки. Політичне життя. 2020. № 1. С. 102-109.

8 Лужицький В. А., Кожухівський А. Д. Основи інформаційної безпеки : навчальний посібник. Вінниця. 2013.

9 Макаренко Є. А., Рижиков М. М., Ожеван М. А., Головченко В. І., Гондюл В. П. Міжнародна інформаційна безпека: Сучасні виклики та загрози. – К.: Центр вільної преси, 2006. – 916 с.

10 Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ:«Гельветика», 2017.168 с.

11 Фролова О.М. Роль ООН в системі міжнародної інформаційної безпеки. URL: http://journals.iir.kiev.ua/index. php/pol_n/article/viewFile/3468/3140 (дата звернення 20.06.2021).

12 Шемчук В.В. Зарубіжний досвід забезпечення інформаційної безпеки держави

13 IEEE/ISO/IEC 8802-1AE-2013 ISO/IEC/IEEE International Standard for Information technology -- Telecommunications and information exchange between systems -- Local and metropolitan area networks -- Part 1AE: Media access control (MAC) security URL:https://ieeexplore.ieee.org/document/6679207 (звернення 12.03.2023)

14 IEEE/ISO/IEC 8802.1AR-2014 ISO/IEC/IEEE International Standard for Information technology -- Telecommunications and information exchange between systems -- Local and metropolitan area networks -- Part 1AR: Secure device identity URL: https://ieeexplore.ieee.org/document/6739984 (звернення 12.03.2023)

15 IEEE/ISO/IEC 8802-11:2018/Amd 1-2019 IEEE/ISO/IEC International Standard - Information technology-Telecommunications and information exchange between systems - Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Fast Initial Link Setup URL: https://ieeexplore.ieee.org/document/8664687 (звернення 12.03.2023)

16 IEEE 802.11-2020 IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications URL: https://ieeexplore.ieee.org/document/9363693 (звернення 12.03.2023)

17 ITU-T X.1054 (04/2021) | ISO/IEC 27014: Information security, cybersecurity and privacy protection - Governance of information security URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14248&lang=en (звернення 10.03.2023)

18 ITU-T X.1052 (10/2020): Information security management processes for telecommunication organizations URL:https://

www.itu.int/ITU-T/recommendations/rec.aspx?rec=14044&lang=en (звернення 10.03.2023)

19 ITU-T X.1631 (07/2015) | ISO/IEC 27017: Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12490&lang=en (звернення 11.03.2023)

20 ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements URL: https://www.iso.org/standard/82875.html (звернення 11.03.2023)

21 ISO/IEC 27019:2017 Information technology — Security techniques — Information security controls for the energy utility industry URL: https://www.iso.org/standard/68091.html (звернення 11.03.2023)

22 ISO/IEC 27006:2015 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems URL: https://www.iso.org/standard/62313.html (звернення 11.03.2023)

23 ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls URL: https://www.iso.org/standard/75652.html (звернення 11.03.2023)

24 ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services URL: https://www.iso.org/standard/43757.html (звернення 10.03.2023)

25 ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection - Guidance on managing information security risks URL: https://www.iso.org/standard/80585.html (звернення 10.03.2023)

26 Cebrovski A., Garstka J. Network–Centric Warfare: Its Origin and Future / A. Cebrovski, J.Garstka // Proceedings. – 1998. – January. URL.: http:// www. kinection. com/ ncoic/ ncw _origin_future.pdf

27 Duncan B. Hollis, Matthew C. Waxman Promoting International Cybersecurity Cooperation: Lessons from the Proliferation Security Initiative (PSI) Temple University Beasley School of Law LEGAL STUDIES RESEARCH PAPER NO. 2018-03 January 26, 2018

28 Francis Lyall International Communications: The International Telecommunication Union and the Universal Postal Union, 2011, page 325

29 Joseph R. Herkert, Christine S. Nielsen Assessing the impact of shift to electronic communication and information dissemination by a professional organization: An analysis of the Institute of Electrical and Electronics Engineers (IEEE),

30 Jonathan Koppell International Organization for Standardization, Handbook of Transnatioal Governance, 2011, pp 289-294

31 Kubo Mačák Is the International Law of Cyber Security in Crisis? 2016 8th International Conference on Cyber Conflict Cyber Power N.Pissanidis, H.Rõigas, M.Veenendaal (Eds.) 2016 © NATO CCD COE Publications, Tallinn

32 Libicki M.C. Conquest in Cyberspace: National Security and Information Warfare / M.C.Libicki. – Cambridge: Cambridge University Press, 2007.–336p.

33 Mazur, M. (2011). The Legal Basis of Informational Security in Face of Modem World Reality or Only a Myth. In: The Academy of Economic Studies of Moldova, Information Security Laboratory, International Conference (8th edition), Security Information 2011. Kishinev, Republic of Moldova, 4 May, Kishinev: Editorial-Polygraphic Department of ASEM, 64–66.

34 Marco Gercke Understanding cybercrime: Phenomena , challenges and LEGAL RESPONSE. International Telecommunication Union Telecommunication Development Bureau Place des Nations CH-1211 Geneva 20 Switzerland

35 Murphy C., Yates J. The International Organization for Standardization (ISO), 2009, page 160

36 Robinson, N., Gaspers, J. (2014). Information Security and Data Protection Legal and Policy Frameworks Applicable to European Union Institutions and Agencies. Brussels: RAND Corporation.

37 Sviatoslav Kavyn, Ivan Bratsuk, Anatoliy Lytvynenko Regulatory and Legal Enforcement of Cyber Security in Countries of the Eu-

ropean Union: The Experience of Germany and France // Teise -2021 –Vol.121 – p.135-147

Sviatoslav Kavyn
Ivan Franko University of Lviv
1 University Street, Lviv, Ukraine, 79000
Postgraduate student, Department of European Law
Faculty of International Relations
Phone: + 380631756263
Email: kavinsviatoslav@gmail.com
ORCID: https://orcid.org/0000-0002-6189-3848

INTERNATIONAL LEGAL REGULATION OF ENSURING INFORMATION SECURITY WITHIN INTERNATIONAL ORGANIZATIONS

The research analyzes the legal mechanisms of international organizations in the field of ensuring information security. There have been reviewed and analyzed legal acts on international information security, which are adopted in the format of international organizations, in particular ITU, IEEE, ISO, and accordingly act as guiding principles for multilateral international relations, taking into account the positions and interests of all international participants. The influence of international organizations on the formation of the legal field of ensuring information security and as a regulator of actions in the field of international informational legal relations is investigated as well. To determine the criteria for evaluating the effectiveness of information protection (level of information security), the work substantiates the application of the methodology of international standards, in particular ISO/IEC, which makes it possible to maximally ensure information protection and minimize information security risks.

On the basis of the conducted research, it is indicated that the formation of a multi-vector environment of legal protection of information requires a systematic approach and, accordingly, the analysis of legal assessments of information security risks, taking into account the peculiarities of informational legal relations in modern conditions of global informatization of society.

Beside this, there is noted in research that since there is still no single legal framework for reliable and effective provision of information security, there is an urgent need to create united standard for information security provision for all structures and organizations under the auspices of a single intergovernmental institution within the framework of international law.

Conducting a comprehensive study of the general patterns of functioning and development of international legal mechanisms for ensuring information security within the framework of the activities of international organizations is particularly relevant and actual, but at the same time requires a detailed analysis.