СЕКЦІЯ 5
ПУБЛІЧНЕ УПРАВЛІННЯ У СФЕРІ ДЕРЖАВНОЇ БЕЗПЕКИ ТА ОХОРОНИ ГРОМАДСЬКОГО ПОРЯДКУ

ЕВОЛЮЦІЯ МІЖНАРОДНО-ПОЛІТИЧНОЇ ВЗАЄМОДІЇ У СФЕРІ ІНФОРМАЦІЙНИХ ВІДНОСИН З ТОЧКИ ЗОРУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

EVOLUTION OF INTERNATIONAL POLITICAL INTERACTION IN THE SPHERE OF INFORMATION RELATIONS FROM THE POINT OF VIEW OF ENSURING INFORMATION SECURITY

УДК 351.86:004.056
DOI https://doi.org/10.32782/pma2663-5240-2023.37.14

Котляров В.О.
докторант кафедри публічного управління та адміністрування
Національний авіаційний університет

У роботі проаналізовано складові елементи інституту міжнародної інформаційної безпеки, ключові аспекти, принципи і підходи до розуміння інформаційної безпеки з позицій міжнародного права, уточнено поняття міжнародної інформаційної безпеки, охарактеризовані моделі міжнародної інформаційної безпеки, організаційна структура забезпечення міжнародної інформаційної безпеки, виявлені особливості забезпечення кібербезпеки.

Автором досліджується зміст категорії «система інформаційної безпеки» та визначаються складові відповідної системи, а також обґрунтовується необхідність розмежування системи інформаційної безпеки та системи забезпечення інформаційної безпеки. Розглянуто нормативно-правовий аспект інформаційної безпеки.

У статті досліджується зміст звіту TCSEC (Trusted Computer System Evaluation Criteria) та документ ITSEC (Information Technology Security Evaluation Criteria). Розглянуто сутність інформаційної безпеки згідно з європейськими критеріями, що включає шість основних елементів деталізації. Обґрунтовано, що важливими мотивами актуалізації проблематики інформаційної безпеки полягають ще й в тому, що тільки країни з розвинутою інформаційною інфраструктурою здатні ставати конкурентоспроможним суб'єктом сучасного міжнародного глобального середовища. У зв'язку з цим, важливим аспектом дослідження різних вимірів інформаційної безпеки держави і суспільства є визначення рівня інформатизації всіх сфер суспільної життєдіяльності.

Виділено чотири складові, що забезпечують інформаційну безпеку. По-перше, законодавча, нормативно-правова та наукова база. По-друге, структура та завдання органів (підрозділів), що забезпечують безпеку ІТ. По-третє, організаційно-технічні та режимні заходи та методи (політика інформаційної безпеки). По-четверте, програмно-технічні способи, і засоби забезпечення інформаційної безпеки.

Ключові слова: *міжнародне правове регулювання, безпека, міжнародна інформаційна безпека, кібербезпека, інформаційні загрози.*

The work analyzes the components of the international institute of information security, of the key issues, principles, elements of the information security from the standpoint of international law, specifies the concept of international information security, characterizes the models of international information security, the organizational structure of ensuring international information security, reveales the peculiarities of cybersecurity.

The author examines the content of the category «information security system» and defines the components of the corresponding system, as well as substantiates the need to distinguish between the information security system and the information security system. The normative and legal aspect of information security is considered.

The article examines the content of the TCSEC (Trusted Computer System Evaluation Criteria) report and the ITSEC (Information Technology Security Evaluation Criteria) document. The essence of information security according to European criteria, which includes six main elements of detail, is considered. It is substantiated that important motives for updating information security issues are also the fact that only countries with a developed information infrastructure are able to become a competitive entity in the modern international global environment. In this regard, an important aspect of the study of various dimensions of information security of the state and society is the determination of the level of informatization of all spheres of public life.

Four components ensuring information security are identified: the first is the legislative, regulatory and scientific base. Secondly, the structure and tasks of bodies (subdivisions) that ensure IT security. Third, organizational, technical and regulatory measures and methods (information security policy). And fourthly, software and technical methods and means of ensuring information security.

Key words: *international legal regulation, security, international information security, cybersecurity, information threats.*

Постановка проблеми у загальному вигляді. Об'єктивно розглядаючи категорію «інформаційна безпека» можна дійти висновку, що вона виникла у той же саме час, що і засоби інформаційних комунікацій між людьми, а також з усвідомленням наявності у людей інтересів, через які з'являється можливість завдати збитків шляхом інформаційних комунікацій, що забезпечують зв'язок між усіма людьми.

В умовах глобалізаційних процесів, зміни міжнародної системи, зміни характеру загроз трансформується і сучасна система загальної безпеки. Простір безпеки трансформується з переважно військового в «комплексне», що включає до себе елементи з суміжних предметних областей світової взаємодії.

Забезпечення національної інформаційної безпеки усередині держави перебуває на стадії розвитку. Це можна пояснити невідповідностями між зміцненням інформаційного суспільства і усвідомленням та потребами у забезпеченні інформаційної безпеки, перед державою постає завдання визначити положення і пріоритет інформаційної безпеки та її захисту в системі ієрархії державних завдань.

У свою чергу, формування єдиної міжнародної системи інформаційної безпеки дозволить в однаковій мірі гарантувати захист національного інформаційного простору кожній державі.

Аналіз публікацій за тематикою дослідження. Дослідженнями інформаційної безпеки займалися В. Беляков, В. Брижко, О. Гальченко, М. Демкова, Л. Задорожня, В. Кирик, А. Крутських, Н. Кушакова-Костицька, А. Леваков, В. Ліпкан, В. Лопатін, К. Макаренко, О. Орєхов, В. Роговець, А. Чорнобров, В. Цимбалюк та інші, але ряд питань, залишилися не висвітленими у науковій літературі. Що стосується дослідження інформаційної безпеки у міжнародному контексті, то можна назвати таких вчених, як Р. Армітідж, П. Б'юкенен, К. Волкер, Дж. Гарст, П. Ізаксон, А. Себровскі, Р. Хартлі, Ю. Хаяші, Е. Хемфрі, К. Шеннон та інших.

Виклад основного матеріалу. Зростаючий інтерес до інформаційної безпеки на сьогоднішній день підтверджується, наприклад, і прийнятим на вищому рівні керівництва НАТО рішенням про посилення уваги до проблеми забезпечення інформаційної безпеки і здатності вести інформаційні війни, обумовленим збільшенням активності потенційних супротивників блоку і прагненням організації відповідати рівню зростаючих загроз кібербезпеки; акцентуванням НАТО на транскордонній природі загроз інформаційній безпеці і проблемах координації дій на наднаціональному рівні; наявністю служб інформації в практично у всіх міжнародних організаціях, у тому числі і військових [1].

«Інформаційна безпека є найважливішою складовою національної безпеки в цілому. Суть цього інституту інформаційного права полягає у здійсненні правових, організаційних, технічних заходів, що забезпечують безпечний стан всіх складових інформаційно-комунікаційного комплексу держави, окремих організацій та кожної людини» [2].

Метою інформаційної безпеки є убезпечення цінності системи, захист і гарантування точності і єдності інформації, мінімізація руйнувань, які можуть мати місце, якщо інформація буде модифікована або знищена. Інформаційна безпека вимагає врахування всіх подій, під час яких інформація створюється, модифікується, до неї забезпечується доступ або вона поширюється [3].

Аналіз наукової літератури, актів права ЄС, міжнародних актів, законодавства України, зарубіжних країн дозволяє виділити кілька основних підходів до змісту поняття інформаційної безпеки:

– поняття інформаційної безпеки як стану інформаційної сфери суспільства (інформаційного середовища суспільства); стан захищеності інформації (інформаційного простору); життєво важливих інтересів особистості, суспільства, держави від різного роду загроз;

– інформаційна безпека тлумачиться як складова національної безпеки. Для цього підходу характерним є поєднання у визначенні понять «стан» і «здатність».

У свою чергу, національна безпека як правове поняття має певну універсальність, що виражає ідею єдності станів безпеки. Ця єдність і служить основою для напрацювання як національних, так і міжнародних правових систем. Тобто, з одного боку, національна безпека характеризується таким важливим фактором, як єдність. При цьому вона завжди поліпредметного. Це протиріччя усувається за засобом правового забезпечення національної безпеки шляхом правового відображення загрози безпеці, її розмірів та законодавчої фіксації способів реагування на загрозу, а також визначенням компетенції органів влади в цьому процесі [4].

У міжнародній практиці виділяються два основні напрями забезпечення інформаційної безпеки. Перший напрям це нормування комп'ютерної безпеки за різними критеріями оцінки захищеності або надійності системи. Інакше кажучи, під цим мається на увазі моніторинг ситуації в інформаційній сфері щодо невиходу за певні, встановлені межі. Другий напрям – це міжнародно-правове регулювання. Якщо розглядати міжнародну взаємодію у межах забезпечення інформаційної безпеки, то за хронологією першим нормативно-правовим документом є документ, підготовлений Агентством комп'ютерної безпеки міністерства оборони США, датований 1983 роком. Воно опублікувало звіт, названий TCSEC (Trusted Computer System Evaluation

Criteria), що перекладається як критерії оцінки захищеності надійних систем. Звіт отримав назву «Помаранчева книга», пов'язано це було з характерним кольором палітурки. У цьому звіті було визначено та розбито в ієрархічному порядку сім рівнів безпеки: A1, B1, B2, B3, C1, C2, D.

Рівень D мав на увазі мінімальну безпеку і був призначений для систем, які були визнані незадовільними. Рівень C має характер виборчого управління доступом. Клас C1 має на увазі низку правил і приписів, таких як: довірена обчислювальна база, повинна виконувати лише об'єкти, які отримали дозволи, захищеність від несанкціонованого доступу, захисні механізми повинні бути в бойовій готовності, повинні бути повністю описані правила безпеки. Клас C2 містить більш точкові доповнення до класу C1. Рівень B, з підкласами B1, B2, B3, які в ієрархічній містять припис до попередніх рівнів. І нарешті рівень A, носить характер повного та гарантованого захисту. Весь цей комплекс розпоряджень був створений з метою проведення загальної оцінки захисту даних, що знаходяться під грифом секретності, в розрахованих на багато користувачів комп'ютерних системах [5].

Для практичної оцінки комп'ютерних систем, Міністерством оборони США та Національним центром комп'ютерної безпеки були підготовлені інструкції NCSC – TG-005 та NCSC-TG-011, більш відомі як червона книга. Паралельно з цим, Агентство інформаційної безпеки Німеччини документ, який називався «Зелена книга», аналогічно названий за кольором палітурки. У цьому документі було розроблено цілий комплекс заходів та вимог до доступності, цілісності та конфіденційності інформації, як у державному, так і у приватному секторі. У 1990 році книга була схвалена цілою низкою європейських країн, такими як сама Німеччина, Великобританія, Нідерланди і Франція, після чого була направлена до Європейського союзу, де на її основі був підготовлений новий документ ITSEC (Information Technology Security Evaluation Criteria) – критерії оцінки захищеності інформаційних технологій. Цей документ також отримав назву за кольором перельоту і був названий «Біла книга». «Біла книга» стала стандартом для європейських держав у питаннях визначення критеріїв, вимог та процедур для створення інформаційних систем з метою забезпечення безпеки, яка, у свою чергу, мала дві схеми оцінки. Перша схема оцінки щодо ефективності, друга за функціональністю і включала доступність системи, її цілісність і конфіденційність інформації та її передачі. «Біла книга» містить основні компоненти безпеки, розроблені в ITSEC. Вона включає такі розділи, як інформаційна безпека, безпека системи, безпека продукту, загроза безпеці, набір функцій безпеки, гарантованість безпеки, загальна оцінка безпеки і класи безпеки [6].

Згідно з європейськими критеріями, інформаційна безпека включає шість основних елементів деталізації.

Перший елемент – це цілі безпеки та функції інформаційної безпеки. Другий елемент має назву специфікації функцій безпеки і має під собою кілька підрозділів. Ідентифікація та автентифікація включає перевірку автентичності користувача, видалення старих користувачів та реєстрацію нових, а також зміни алгоритму автентифікації та обмеження повторних спроб [7].

Другий елемент відповідає за керування доступом. Інші розділи відповідають за звітність, аудит, точність інформації, обслуговування та обмін даних. Крім цього, у «Білій книзі» проводиться розмежування понять система та продукт. Система – це конкретна апаратно-програмна конфігурація, створена з цілком певними цілями і працює у відомому оточенні. Продукт, у свою чергу, мається на увазі апаратно-програмний пакет, що доступний для покупки, і після цього власник може вставити його в ту чи іншу систему. Для об'єднання критеріїв оцінки системи та продукту було прийнято рішення, в рамках «білої книги», запровадити єдиний термін «об'єкт» оцінки [8].

Кожна система чи продукт висувають свої вимоги до організаційних моментів забезпечення інформаційної безпеки. Ними є елементи, перелічені вище. Відповідно, для кожного продукту чи системи вони підбираються індивідуально. У Європейських умовах безпеки, на відміну від критеріїв безпеки встановлених у США, було встановлено десять рівнів. Вони отримали порядкові номери F-C1, F-C2, F-1, F-B2, F-B3, F-1N, F-AV, F-DI, F-DC, F-DX. Перші п'ять із ідентичних рівнів з американського документа. Клас F-1N був призначений для систем, які залежать від забезпечення їх цілісності. Це мало на увазі читання, запис, додавання, видалення, створення, перейменування та виділення об'єктів. Клас F-AV був призначений для систем з високими вимогами до забезпечення їхньої працездатності за рахунок протидії загрозам відмови в обслуговуванні. Клас F-DI був орієнтований на системи з підвищеними вимогами до цілісності даних, що передаються каналами зв'язку. Клас F-DC характеризувався підвищеними вимогами до конфіденційності інформації, а клас F-DX призначений для систем з підвищеними вимогами одночасно за класами F-DI та F-DC. Основним методом регулювання інформаційної безпеки в рамках міжнародного співробітництва є метод міжнародно-правового регулювання [9].

До основних аспектів міжнародно-правового регулювання насамперед відносяться норми міжнародного права. Основну функцію регулювання належать до норм міжнародного гуманітарного права. У його межах встановлюються правила ведення воєнних дій, у межах воєнних конфліктів, а також регулювання відносин в інформаційній сфері.

Найважливішим міжнародним актом, у межах міжнародного права, є «Окінавська Хартія глобального інформаційного суспільства». Вона включає 19 пунктів і розбита на кілька розділів. Перший відповідає питання про мотивацію створення цього документа і позначають важливість інформаційних технологій у світі, що змінюється. Другий розділ визначає спектр використання інформаційних технологій. Третій виносить проблему інформаційно-цифрового розриву і містить у собі план його вирішення. Заключні розділи містять план сприяння між країнами та перспективи подальшого розвитку.

Не менш важливими документами є «Декларація про європейську політику в галузі нових інформаційних технологій». Цей документ складено, як наслідок прийнятої резолюції ООН, Резолюцію 53/70 Генеральної Асамблеї ООН (грудень 1998 р.) і містить розпорядження, у рамках концепції розвитку нового інформаційного суспільства. Також до одним із найважливіших документів, у цій галузі є «Декларація Комітету міністрів з прав людини і верховенства права в Інформаційному Товаристві». У цьому документі прописані, як випливає із назви документа, права людини. Основними пунктами документа є право на свободу вираження, повагу до приватного життя у листуванні тощо. Також було зроблено спроби розглянути інформаційну безпеку в рамках кримінального права. На міжнародному рівні, першу спробу було здійснено «Організацією економічного співробітництва та розвитку» (ОЕСР), у 1986 році. Подібну ініціативу розглядав Комітет міністрів країн-членів Європи в 1989 році. На жаль, через низку обставин будь-яких реальних результатів, ці дії не отримали, оскільки вони мали характер першопрохідників у цій галузі [10].

У 1996 році було прийнято модельний кримінальний кодекс для країн-учасниць СНД. У цьому кримінальному кодексі розділ XII був повністю присвячений інформаційній безпеці. Цей розділ включав сім статей: несанкціонований доступ до комп'ютерної інформації, модифікація комп'ютерної інформації, комп'ютерний саботаж, неправомірне заволодіння комп'ютерною інформацією, виготовлення та збут спеціальних засобів для отримання неправомірного доступу до комп'ютерної системи або мережі, розробка, використання та розповсюдження шкідливих програм, порушення правил експлуатації комп'ютерної системи чи мережі.

І нарешті, було прийнято Конвенцію Ради Європи про злочинність у сфері комп'ютерної інформації від 23 листопада 2001 р. На жаль, ці кроки не призвели до позитивного впливу на боротьбу з кіберзлочинністю. Справа в тому, що злочини, пов'язані з інформацією, відображені на цифрових носіях, вони мають свою особливу специфіку. Іншими словами, відбувається постійний технологічний розвиток, способи скоєння злочинів стають більш витонченими і у зв'язку з цим нормативні акти не здатні врівноважити загрозу, що постійно модифікується. Як зазначають деякі науковці «транскордонний характер таких злочинів, труднощі їх локалізації та доведення в судах стимулювали розвиток практики комплексного забезпечення інформаційної безпеки на основі відомчих, галузевих, національних та міжнародних стандартів, які почали динамічно розроблятися та кругом використовуватись» [11].

У зв'язку з цим було створено Міжнародну Електротехнічну Комісію (МЕК) та Міжнародної Організації зі Стандартизації (МОС). Це міжнародні професійні об'єднання. Їх відмінними рисами є те, що вони наголошують не тільки на вирішенні проблем забезпечення інформаційної безпеки. Ця проблема, як правило, вирішується разом з іншими проблемами, такими як розвиток інформаційних технологій, побудова телекомунікаційних систем та інші проблеми технологічного характеру. Так само відмінною особливістю таких організацій є опора на підтримку різних державних структур. Тобто, різні держави найчастіше оформляють у подібних організацій замовлення, які вони виконують. Про це свідчить і характер зайнятості працівників у подібних організаціях. Вони можуть мати конкретних зобов'язань всередині організації, під час виконання роботи. Таких організацій, на даний момент, досить багато і багато хто з них має майже вікову історію. Міжнародна Електротехнічна Комісія (МЕК) є міжнародною некомерційною організацією зі стандартизації у галузі електричних, електронних та суміжних технологій. На сьогоднішній день членами цієї організації є 60 країн. Свої стандарти в галузі інформаційних технологій організація часто створює спільно з Міжнародною організацією зі стандартизації. Ця організація, у свою чергу, займається аналогічною діяльністю, за винятком питань, відведених виключно Міжнародній Електронній Комісії, і налічує понад 100 комітетів – членів.

Висновки та перспективи подальших розвідок. Таким чином, виділяється чотири складові, які забезпечують інформаційну безпеку та які були описані у даній статті. По-перше, це законодавча, нормативно-правова та наукова база. По-друге, структура та завдання органів (підрозділів), що забезпечують безпеку ІТ. По-третє, організаційно-технічні та режимні заходи та методи (політика інформаційної безпеки). І по-четверте, програмно-технічні способи, і засоби забезпечення інформаційної безпеки.

Можна виділити такі моделі системи глобальної інформаційної безпеки:

– модель 1 – створення абсолютної системи захисту країни-інформаційного лідера (дана модель конструюється залежно від кількості суб'єктів системи безпеки, відповідно виділяються чотири основні моделі, що конкурують між собою: однополярна система безпеки, «концерт держав», багатополярна модель, глобальна (універсальна) модель);

– модель 2 – створення значної переваги держави-потенційного ініціатора інформаційної війни;

– модель 3 – наявність кількох країн-інфолідерів та потенційного протиборства між ними;

– модель 4 – всі конфліктуючі сторони використовують транспарентність інформації для формування ситуативних альянсів.

У свою чергу, ці напрями покликані вирішувати ряд завдань: заборона розробки, розповсюдження та застосування «інформаційної зброї», забезпечення безпеки міжнародного обміну інформацією, підвищення захисту інтелектуальної власності, запобігання несанкціонованому доступу до конфіденційної інформації тощо. Отже, слід зазначити, що всі перелічені напрями міжнародної взаємодії у сфері забезпечення інформаційної безпеки є важливими напрямами у цій галузі [12].

Забезпечення прав і безпеки суб'єктів інформаційної взаємодії – як національного, транскордонного, міжнародного, можливе лише на основі спільного комплексного вирішення правових, організаційних і технологічних питань, для чого необхідно прийняти міжнародні правила (кодекс) поведінки в глобальному інформаційному просторі або універсальну конвенцію під егідою ООН.

ЛІТЕРАТУРА:

1. Васенко В.К., Тереніна О.В. Безпека життєдіяльності та її особливості у правоохоронних органах. *Право і безпека.* 2012. № 1. С.213–217.

2. Брижко В.Н., Гальченко О.М., Цимбалюк В.С., Орєхов О.А., Чорнобров А.М. Інформаційне суспільство. Дефініції: людина, її права, інформація. *Інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок, юриспруденція*. К., 2002. 523 с.

3. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції: навч. посіб. Київ: КНТ, 2006. 280 с.

4. Хемфрі Е. Діяльність з кібербезпеки. Рішення для бізнесу. *Стандартизація. Сертифікація. Якість*. 2013. №1. С. 16–18.

5. Кузнецов А.В. Спосіб визначення реєстрованих. *Питання кібербезпеки.* 2015. №13. С. 23–25.

6. Файчук О.В., Лещенко М.А., Ткач Д.Е. Інформаційна безпека як індикатор стабільності страхового ринку України. *Правове регулювання фінансових послуг: національний, європейський, глобалізаційний виміри.* 2022. С. 94.

7. Макаренко А.О. Аналіз оцінки поточного стану інформаційної безпеки на основі SIEM-систем. Інформаційна безпека та інформаційні технології. 2020. С. 13–14.

8. Малик Я. Інформаційна війна і Україна. *Демократичне врядування.* 2015. Вип. 15. URL: http://nbuv.gov.ua/UJRN/DeVr_2015_15_3 (дата звернення: 10.10.2022).

9. Киричок Р.В., Складанний П.М., Бурячок В.Л., Гулак Г.М., Козачок В.А. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення. *Наукові записки Українського науково-дослідного інституту зв'язку.* № 3, 2016. С. 48–61.

10. Коваль О.В. Узагальнена архітектура аналітичної складової корпоративних інформаційно-аналітичних систем. *Реєстрація, зберігання і обробка даних*. № 13(2), 2021. С. 53–73.

11. Носов В., Манжай О. Окремі аспекти протидії інформаційної війни в Україні. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: науково-технічний збірник.* 2015. Вип. 1. С. 26–32.

12. Про основні засади забезпечення кібербезпеки України, Закон України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення 01.04.2022).

13. Інформаційні війни та майбутнє України. *Бюлетень СІАЦ.* URL: http://siac.com.ua/index.php?option=com_content&task=category&sectionid=8&id=129&Itemid=44 (дата звернення: 23.10.2022).

14. Інформаційні війни. URL: http://pidruchniki.com/18000102/ politologiya/informatsiyni_viyni (дата звернення: 22.09.2022).

15. Danko Y. I. & Reznik N. P. (2019). Contemporary challenges for China and Ukraine and perspectives for overcoming these challenges. *Global Trade and Customs Journal*, 14(6).

16. Reznik N., Hridin O., Chukina I., Krasnorutskyy O., Mykhaylichenko M. (2022). Mechanisms and tools of personnel management in institutional economics. *AIP Conference Proceedings.* 2413, 040012 https://doi.org/10.1063/5.0089330.