Міністерство освіти і науки України
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»
Білостоцький технологічний університет (Польща)
Вроцлавський економічний університет (Польща)
Гентський університет (Бельгія)
UNIVERSITY ISMA (Латвійська республіка)
UNIVERSITY NORTH (Хорватія)
VARNA FREE UNIVERSITY «CHERNORIZETS HRABAR» (Болгарія)
Академія праці, соціальних відносин та туризму
Міжрегіональна Академія управління персоналом
Національний технічний університет «Дніпровська політехніка»
Національний університет «Чернігівська політехніка»
Тернопільський національний технічний університет імені Івана Пулюя
Хмельницький університет управління та права імені Леоніда Юзькова
Івано-Франківський національний технічний університет нафти і газу
Черкаський національний університет імені Богдана Хмельницького

ОРГАНІЗАЦІЙНО-ПРАВОВІ АСПЕКТИ ПУБЛІЧНОГО УПРАВЛІННЯ В УКРАЇНІ

Матеріали XI Міжнародної науково-практичної Інтернет-конференції

25 квітня 2024 року

Полтава – 2024

не вдосконалення процесів діловодства стають основою для забезпечення якості та ефективності управління в органах виконавчої влади.

Література:

1. Асанова Л. Місце електронного документообігу в загальній системі діловодства. *Адміністративне право і процес.* Вип. № 3. 2021. С. 156-160. URL: http://pgp-journal.kiev.ua/archive/2021/3/25.pdf

2. Публічне управління: український вимір : матеріали щорічної наук.-практ. конференції, 7 грудня 2022 р., м. Харків; електронне видання. Харків : ХНУ імені В. Н. Каразіна. 2023. 176 с. URL: https://ipa.karazin.ua/wp-content/themes/education/filesforpages/science/Zbirnik_za%20materialami%20konferenciyi_7_grudnya%202022%20_2.pdf

3. Трофімук-Кирилова Т., Карпюк А. Організація роботи з документами як складова управлінських процесів в органах місцевого самоврядування. *Економіка та суспільство*. Вип. № 57. 2023. с. 9. URL: https://economyandsociety.in.ua/index.php/journal/article/view/3238/3161

Кульчій Інна Олексіївна

Національний університет «Полтавська політехніка імені Юрія Кондратюка», завідувачка кафедрою публічного управління, адміністрування та права, кандидат наук з державного управління, доцент

АДАПТАЦІЯ ДОСВІДУ КРАЇН ЄС ІЗ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Аналізуючи досвід країн ЄС із системи забезпечення інформаційної безпеки, варто зауважити, що пошук певного балансу між повним державним контролем і ринковими законами, тобто поєднанням влади та ринкових сил, є головною ознакою інформаційної політики не лише в Північній Європі, а й в інших країнах Європейського Союзу. У той же час ЄС продовжує приділяти пильну увагу сьогодні приватизації та лібералізації ринку інформаційно-комунікаційних технологій. Процес глобалізації та боротьби з тероризмом привели до розробки нової концепції стратегії національної безпеки, яка безперешкодно поєднує політику оборони, політику внутрішньої безпеки, зовнішню та економічну політику.

«Залежність від комунальних інформаційних систем, транспортної інфраструктури, продовольчої безпеки та навіть управління обороною робить сучасне суспільство та його безпеку вразливими для випадкових пошкоджень та цільових атак з боку комп'ютерних мереж. Загроза шпигунства та стратегічного впливу виправдовується широким використанням (м'якої сили) у міждержавних відносинах, маніпулюванням свідомістю через ЗМІ та Інтернет, досягненням наукового, економічного, оборонного потенціалу Франції та її території, небезпека культурної експансії» [10. с. 456.].

Defense Review приділяє значну увагу «інформаційним загрозам та заходам протидії. Таким чином, зазначається, що в кіберпросторі деякі атаки через їх масштаби і серйозність можуть бути класифіковані як озброєна агресія. Труднощі з розподілом часток та поєднанням прямої дії з методами впливу та пропаганди дозволяють використовувати численні інструментальні сценарії для дестабілізації або підтримки більш простих операцій.

Крім того, для забезпечення безпеки інформації Defense Review допускає кібервійну, що означає оборонну або наступальну боротьбу у всьому цифровому середовищі проти урядових чи неурядових супротивників.

Наприклад, система інформаційної безпеки у Франції складається з таких спеціальних структур «Національного агентства з безпеки інформаційних систем (ANSSI)», «Аудіовізуальної служби (Audiovisual), Міжвідомчого управління інформаційних систем та комунікацій (DISIC)», «Управління розвитку ЗМІ)» та інші деякі. ANSSI відповідає за просування національних технологій, систем та досвіду для просування цифрової економіки. При цьому основні зусилля фахівців ANSSI спрямовані на реалізацію заходів, передбачених у стратегії національної безпеки та оборони. «Основними завданнями агенції є підвищення ефективності управління та координації органів державної влади, критичної інфраструктури, суспільства з погляду комп'ютеризації; забезпечення промислової безпеки, організація захисту національної розвідувальної та телекомунікаційної інфраструктури в умовах військової загрози, у тому числі кібервійни; підтримка технічних засобів, необхідних для виконання завдань, поставлених перед Агентством у його нинішньому вигляді. Аудіовізуальна служба, яка діє під головуванням президента, також бере участь у реалізації інформаційної політики у Франції. Служба розробляє аудіовізуальні технічні платформи Президента Республіки, організує його виступи та забезпечує їх поширення по всій країні та за кордоном».

Основним законом у галузі інформаційної безпеки у Німеччині є Закон «Про посилення безпеки систем інформаційних технологій» (Information Security Law) від 25.07.2015. Закон відводить Федеральному управлінню інформаційних технологій (BSI) центральну роль захисту критично важливої інфраструктури у Німеччині. Критичні інфраструктури – це установки, установки або їх частини, які «належать до секторів енергетики, інформаційних технологій та телекомунікацій, транспорту та дорожнього транспорту, охорони здоров'я, водопостачання, продовольства, фінансів та страхування. Такі об'єкти важливі для функціонування спільноти, оскільки їх закриття або погіршення стану спричинить значний брак матеріалів або створить загрозу громадській безпеці. 27 березня 2019 року Федеральне міністерство внутрішніх справ також опублікувало законопроект щодо безпеки інформаційних технологій, який містить цілісний підхід до безпеки у цій сфері.

Серед іншого, «передбачається запровадити простий у використанні ярлик комп'ютерної безпеки для комерційних продуктів, а також посилити компетенцію BSI та розширити список порушень кібербезпеки та пов'язаних із ними слідчих дій. Законопроект також збільшує кількість отримувачів звітів та зобов'язань. Загалом очікується, що закон створить певні економічні труднощі для підприємств та органів державної влади» [57].

«Інформаційна безпека у Німеччині забезпечується Федеральними збройними силами Німеччини (Бундесвер), зокрема, Відділом комп'ютерних мереж та інформаційних операцій Командування стратегічної розвідки. Командування стратегічної розвідки також керує системою розпізнавання супутників SAR-Lupe [4]. Завдяки п'яти супутникам SAR-Lupe, які вважаються одними з найпередовіших систем у своєму роді, може передаватися зображення з роздільною здатністю менше одного метра, незалежно від денного світла та погоди. Таким чином, можна прояснити практично будь-яку точку Землі. Система збирає та оцінює інформацію про військово-політичну ситуацію в окремих країнах та альянсах потенційного чи поточного супротивника та його збройних сил.

Отже, проаналізувавши досвід Країни ЄС щодо системи інформаційної безпеки варто відмітити, що на сьогодні немає універсального підходу чи єдиної моделі управління інформаційної безпекою. У кожного регіону світу та країни є свої внутрішні особливості, які надалі визначають специфіку цього процесу. Системи інформаційної безпеки у Франції та Німеччині засновані на усвідомленні ризиків та загроз, пов'язаних із швидким розвитком інформаційних та комунікаційних технологій. Наприклад, одним з основних гравців у системі інформаційної безпеки у Франції є Національне агентство безпеки інформаційних систем (ANSSI), а в Німеччині – Управління інформаційних та комп'ютерних мереж Бундесверу.

Література:

1. Антонюк В.В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України. Дисертація на здобуття наукового ступеня кандидата наук з державного управління. 25.00.02. Механізми державного управління. Національна академія державного управління при Президентові України. Київ. 2017. 218 с.

2. Березовська І. Р. Суб'єкти у сфері забезпечення інформаційної безпеки в Україні. Наукові записки Львівського університету бізнесу та права. 2023. Вип. 10. С. 148-153.

3. Котляров В. Основні підходи у концепції інформаційної безпеки. Актуальні питання у сучасній науці. 2023. № 1(7). URL: https://doi.org/10.52058/2786-6300-2023-1(7)-474-484 (дата звернення: 9.04.2024).записки Львівського університету бізнесу та права. 2013. Вип. 10. С. 148-153.