Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Інститут цифровізації освіти НАПН України
Національний технічний університет України
«Київський політехнічний інститут» ім. І. Сікорського
Вінницький національний технічний університет
Житомирський військовий інститут імені С.П. Корольова
Тернопільський національний технічний університет імені Івана Пулюя
Харківський національний університет радіоелектроніки
Уманський державний педагогічний університет імені Павла Тичини
Національний університет біоресурсів і природокористування України
Інститут геохімії навколишнього середовища НАН України
Черкаський державний технологічний університет
Державний університет «Київський авіаційний інститут»

Комп'ютерні технології: інновації, проблеми, рішення

Тези доповідей VIII Всеукраїнської науково-технічної конференції

м. Житомир, 02-03 грудня 2025 р.

2025

УДК 35:004.056.5

Бень Д.Ю., здобувач,
Ткачук Р.Л., д.т.н., професор,
Ящук В.І., к.екон.н., доцент
Львівський державний університет безпеки життєдіяльності

АДМІНІСТРАТИВНО-ПРАВОВІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ДЕРЖАВИ

Стрімка цифровізація та зростання кіберзагроз, особливо в умовах гібридної агресії проти України, роблять критично важливим ефективне адміністративно-правове врегулювання діяльності суб'єктів сектору безпеки і оборони, оскільки узгодженість їхніх повноважень визначає здатність держави забезпечувати кіберстійкість та оперативно реагувати на кіберінциденти.

Нормативно-правову основу формують Закон України «Про основні засади забезпечення кібербезпеки України» (2017), Закон України «Про національну безпеку України» (2018), Стратегія кібербезпеки України (2021), Закон України «Про основи національного спротиву» (2021), а також численні підзаконні акти: Положення про Держспецзв'язку, Положення про Службу безпеки України, нормативи НЦКБ при РНБО. Попри розширення нормативного масиву, чинне законодавство все ще містить колізії й прогалини, що стосуються розмежування функцій державних органів. Найбільш проблемними є питання дублювання повноважень між Держспецзв'язку (як технічним регулятором), СБУ (як контррозвідувальним органом), Кіберполіцією та Міністерством оборони. Невизначеність меж компетенції створює «сірі зони» у державному управлінні, що негативно впливає на координацію та швидкість реагування на кіберінциденти.

Особливого значення набуває уточнення адміністративно-правового статусу суб'єктів сектору безпеки в умовах воєнного стану, оскільки ефективність протидії кібератакам (WhisperGate, HermeticWiper, NotPetya, Deface 2022–2024) залежить насамперед від чіткості алгоритмів взаємодії та нормативного визначення компетенції органів.

Дослідження зосереджувалося на комплексному адміністративно-правовому аналізі статусу та компетенції суб'єктів сектору безпеки і оборони у сфері кібербезпеки з урахуванням національного законодавства, галузевих стандартів і міжнародних підходів НАТО та ЄС. Особлива увага приділяється нормативно-правовим механізмам організації кіберзахисту та розподілу повноважень між СБУ, Держспецзв'язку, НЦКБ, Міноборони та іншими ключовими суб'єктами.

На підставі проведених досліджень, на нашу думку, ключові проблемні аспекти можна сформулювати наступним чином:

– відсутність чіткого розмежування між функціями кіберзахисту (Держспецзв'язку), кіберрозвідки та контррозвідки (СБУ, ГУР МОУ) створює правові прогалини, які можуть бути використані противником;

– діяльність НЦКБ потребує розширення адміністративно-правових механізмів впливу та підпорядкування єдиній вертикалі рішень щодо реагування на критичні кіберінциденти;

– євроатлантична інтеграція має охоплювати не лише технічну, а й правову сумісність із підходами НАТО, зокрема відповідно до NATO Cyber Defence Policy, Tallinn Manual 2.0, EU Cybersecurity Act та Директиви NIS2.

Таким чином, удосконалення адміністративно-правових механізмів, усунення законодавчих колізій та впровадження єдиного стратегічного підходу до міжвідомчої координації є ключовим для формування ефективної та стійкої системи кіберзахисту України. Це забезпечує чітке визначення компетенцій органів, оперативне реагування на загрози та гармонізацію національних стандартів із практиками НАТО та ЄС.

Список використаних джерел:

1. Законодавство України. Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua

2. Regulation (EU) 2019/881 of the European Parliament and of the Council «Cybersecurity Act». URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj

3. NATO. Comprehensive Cyber Defence Policy. 2021. URL: https://www.act.nato.int/activities/cyber/

4. NATO. How NATO-Accredited Cyber Defence Centre of Excellence Advances Legal Interoperability. 2025. URL: https://www.act.nato.int/article/ccdcoe-2025/

5. Івануса А. І., Ткачук Р. Л., Брич Т. Б. Удосконалення методів управління процесами інформаційної безпеки // Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану : матеріали III Міжнар. наук.-практ. конф., Хмельницький, 21 листопада 2024 р. Хмельницький : НАДПСУ, 2024. С. 1136–1138.