

Сергій Моторин,
здобувач ТДАТУ, Керівник: **Ганна Ортіна**
доктор наук з державного управління,
кафедра менеджменту та публічного адміністрування,
Таврійський державний агротехнологічний університет
імені Дмитра Моторного,
м. Запоріжжя, Україна

CYBER RESILIENCE GOVERNANCE У СИСТЕМІ ESG-БЕЗПЕКИ ТЕРИТОРІАЛЬНИХ ГРОМАД

Актуальність дослідження. Цифровізація системи публічного управління створює нові можливості для розвитку територіальних громад, однак одночасно формує масштабні кіберризики, пов'язані із захистом інформаційної інфраструктури, безпекою цифрових сервісів та стійкістю систем governance до зовнішніх загроз. У сучасних умовах територіальні громади дедалі активніше використовують електронне врядування, цифрові реєстри, автоматизовані системи управління та онлайн-платформи взаємодії з населенням. Це актуалізує проблему формування cyber resilience governance як складової сучасної ESG-oriented public security policy.

Післявоєнне відновлення України супроводжується значним зростанням залежності системи публічного управління від цифрової інфраструктури. У цих умовах кібератаки на системи місцевого самоврядування, цифрові реєстри, комунальні сервіси та інформаційні мережі можуть становити серйозну загрозу для стабільності територіальних громад. Саме тому cyber resilience сьогодні розглядається як важлива складова strategic governance та безпекової політики держави.

У сучасному міжнародному дискурсі ESG increasingly інтегрується у систему security governance та risk management. Governance-компонент ESG сьогодні охоплює не лише прозорість чи підзвітність, а й інформаційну безпеку, цифрову стійкість, захист критичної інфраструктури та антикризове управління. У цьому контексті cyber resilience governance виступає важливим механізмом забезпечення institutional stability та continuity management у системі public administration.

Важливим елементом cyber resilience governance є формування системи proactive risk management. На відміну від традиційного реагування на кіберінциденти, сучасна модель governance повинна базуватися на прогнозуванні ризиків, превентивному моніторингу цифрових загроз та інтеграції cyber security policy у систему strategic planning територіальних громад. У сучасних умовах територіальні громади повинні формувати cyber resilience strategies, орієнтовані на забезпечення безперервності функціонування critical public services.

Особливого значення набуває захист цифрової інфраструктури місцевого самоврядування. Smart infrastructure systems, електронні сервіси, цифрові архіви, GIS-платформи та системи електронної демократії виступають ключовими елементами сучасного public governance. Порушення функціонування таких систем

може призводити до дестабілізації управлінських процесів, втрати даних та зниження рівня суспільної довіри до органів влади.

Соціальний вимір cyber resilience governance пов'язаний із формуванням цифрової грамотності населення та підвищенням рівня cyber awareness у громадах. У сучасних умовах інформаційна безпека дедалі більше залежить від рівня обізнаності громадян щодо цифрових ризиків, захисту персональних даних та безпечного використання цифрових сервісів. Саме тому органи місцевого самоврядування повинні реалізовувати educational cyber programs та community cyber resilience initiatives.

Важливу роль у системі ESG-security governance відіграє міжінституційна координація. Ефективне cyber governance потребує взаємодії органів місцевого самоврядування, державних структур, ІТ-сектору, громадських організацій та міжнародних партнерів. У сучасному європейському просторі collaborative cyber governance виступає одним із ключових механізмів забезпечення digital resilience та security sustainability.

У сучасних умовах післявоєнного recovery governance особливої актуальності набуває питання захисту цифрових систем управління міжнародною допомогою та recovery monitoring systems. Прозорість використання фінансових ресурсів, безпечне функціонування цифрових платформ та захист даних є важливими передумовами ефективного recovery management та міжнародної довіри до системи governance України.

Таким чином, cyber resilience governance виступає важливим напрямом модернізації системи public security governance територіальних громад. Інтеграція ESG-principles, cyber risk management та digital security policy створює передумови для формування стійких, адаптивних та безпечних моделей territorial governance в умовах цифрової трансформації та післявоєнного відновлення.

Висновки. У результаті дослідження встановлено, що cyber resilience governance виступає важливою складовою сучасної ESG-oriented security policy територіальних громад. Обґрунтовано необхідність інтеграції механізмів cyber security, proactive risk management та digital resilience у систему strategic public governance. Визначено, що розвиток cyber resilience communities сприяє підвищенню стійкості цифрової інфраструктури, безпеки public services та ефективності crisis management. Доведено, що cyber resilience governance виступає перспективним напрямом модернізації системи territorial governance України відповідно до сучасних європейських стандартів digital security та sustainable governance.

Список використаних джерел

1. Cavelty M. D. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. London : Routledge, 2008. 198 p.
2. European Union Agency for Cybersecurity (ENISA). *Cybersecurity and Resilience of Smart Cities*. Brussels, 2022. 94 p.
3. Dunn Cavelty M., Wenger A. *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*. London : Routledge, 2020. 276 p.

4. OECD. *Digital Security Risk Management for Economic and Social Prosperity*. Paris : OECD Publishing, 2015. 180 p.
5. United Nations. *Transforming our world: the 2030 Agenda for Sustainable Development*. New York : UN, 2015. 41 p.
6. European Commission. *The EU Cybersecurity Strategy for the Digital Decade*. Brussels, 2020. 32 p.
7. World Economic Forum. *Global Cybersecurity Outlook 2024*. Geneva : WEF, 2024. 118 p.