

КІБЕРНЕТИЧНА БЕЗПЕКА В ПОЛІТИЦІ УКРАЇНИ

Вінницький національний технічний університет

Анотація

Досліджено феномен кібернетичної безпеки як складової державної політики України. Визначено її роль у забезпеченні національних інтересів, захисті демократичних процесів та інтеграції в європейський і євроатлантичний простір. Проаналізовано чинну нормативно-правову базу, функції державних інституцій, сучасні тенденції у сфері кіберзахисту та основні загрози, зокрема гібридні кібератаки, дезінформаційні кампанії та втручання у виборчі процеси. Розкрито особливості міжнародної співпраці України у сфері кібербезпеки, а також запропоновано напрями вдосконалення державної політики.

Ключові слова: кібернетична безпека, політика України, інформаційні загрози, правове регулювання, міжнародна співпраця.

Abstract

The study examines cyber security as a component of Ukraine's national policy. It identifies its role in safeguarding national interests, protecting democratic processes, and integrating into the European and Euro-Atlantic space. The analysis covers the current regulatory framework, the responsibilities of government agencies, emerging trends in cyber defense, and major threats such as hybrid cyberattacks, disinformation campaigns, and interference in electoral processes. It highlights the unique aspects of Ukraine's international cooperation in cybersecurity and suggests ways to enhance government policy.

Keywords: cybersecurity, Ukrainian policy, information threats, legal regulation, international cooperation.

Вступ

Сучасна політика України функціонує в умовах глобалізованого інформаційного простору, де кіберзагрози стають одним із головних чинників дестабілізації. Актуальність проблеми кібернетичної безпеки зумовлена як внутрішніми, так і зовнішніми викликами. З одного боку, цифровізація державних послуг, електронне врядування, розвиток онлайн-комунікацій сприяють демократизації та відкритості політичної системи. З іншого — вони роблять державу та суспільство більш вразливими до кібератак, маніпуляцій та інформаційних диверсій.

Кібербезпека у політиці України має багатовимірний характер. Вона охоплює захист критичної інформаційної інфраструктури, забезпечення безперебійної роботи державних інституцій, недопущення втручання у виборчі процеси, протидію поширенню фейкових новин та інформаційних маніпуляцій, а також розвиток міжнародного партнерства у сфері кіберзахисту.

Основна частина

Ключовим нормативним актом, що регулює цю сферу, є Закон України «Про основні засади забезпечення кібербезпеки України» (2017 р.), який визначає базові принципи, суб'єкти та напрями кіберзахисту. Закон закріплює роль держави як гаранта безпеки інформаційного простору, проте одночасно передбачає взаємодію з приватним сектором та міжнародними організаціями. Серед інституційних механізмів важливе місце посідають Державна служба спеціального зв'язку та захисту інформації України, Національний центр кібербезпеки при РНБО, урядова команда реагування на комп'ютерні надзвичайні події CERT-UA. Їх діяльність спрямована на моніторинг інцидентів, розробку стратегій та проведення навчань [2, с. 45].

Проблемою залишається дублювання повноважень різних органів та нестача належної координації. Наприклад, у випадках масштабних кібератак на державні установи чи енергетичну інфраструктуру, що відбувалися у 2015–2022 роках, державна реакція була ускладнена відсутністю єдиного кризового центру оперативного реагування.

Особливу небезпеку становить вплив кіберзагроз на політичні процеси. Поширення дезінформації, маніпуляцій у соціальних мережах та хакерських атак під час виборчих кампаній загрожує

легітимності демократичних інститутів. Дослідження фіксують активне використання технологій «ботоферм», фейкових сторінок та цілеспрямованих інформаційних атак з боку іноземних держав для формування негативного іміджу української влади та дестабілізації суспільної думки [3, с. 78].

Міжнародний вимір кібербезпеки є одним із ключових у політиці України. Важливими напрямками є співпраця з НАТО, участь у програмах ЄС, долучення до Будапештської конвенції про кіберзлочинність. Позитивним прикладом є проведення спільних навчань «Cyber Coalition» у межах НАТО, що дозволяють вдосконалити координацію та відпрацювати реагування на кіберзагрози [4, с. 109].

Водночас залишаються невирішеними кадрові проблеми у сфері кіберзахисту. Недостатня кількість висококваліфікованих фахівців у державних структурах призводить до залежності від зовнішніх підрядників. Серед викликів також — обмежене фінансування, відсутність цілісної системи освіти у сфері кіберполітики та нерівномірний рівень цифрової грамотності громадян.

Висновки

Кібернетична безпека посідає ключове місце у політиці України, адже від її ефективності залежить не лише стабільність внутрішньополітичної системи, а й міжнародний авторитет держави. У сучасних умовах гібридної війни та зростання кількості кібератак саме надійна кіберзахисна політика стає запорукою збереження державного суверенітету та демократичного розвитку. Попри наявність нормативно-правової бази та функціонування спеціалізованих державних інституцій, ця сфера й надалі потребує вдосконалення, зокрема чіткішої координації між органами влади, розвитку єдиного центру кризового реагування, розширення кадрового потенціалу та фінансування. Важливим завданням є також формування в суспільстві культури цифрової грамотності, що сприятиме підвищенню стійкості громадян до інформаційних маніпуляцій. Удосконалення державної політики у сфері кібербезпеки, посилення міжнародної співпраці та інтеграція в європейські й євроатлантичні стандарти дозволять Україні не лише ефективно протистояти сучасним кіберзагрозам, але й зміцнити політичну систему, забезпечити прозорість та довіру громадян до влади, а також створити передумови для сталого розвитку в умовах глобальних викликів цифрової епохи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Завгородня Ю. В. Кібербезпека як інноваційний захист у політичному просторі України. Вісник НТУУ «КПІ». Політологія. 2023. №1. С. 14–19.
2. Закон України «Про основні засади забезпечення кібербезпеки України». *Відомості Верховної Ради України*. 2017. № 45.
3. Бурячок В. Л. Інформаційна безпека та кіберзахист в умовах гібридної війни. Київ : КНТ, 2019. 215 с.
4. NATO Cooperative Cyber Defence Centre of Excellence. Annual Report 2022. Tallinn: NATO CCDCOE, 2022. 134 с.
5. IFES Ukraine. Cybersecurity Legal Framework in Ukraine. Kyiv, 2021. 52 с.
6. Державна служба спеціального зв'язку та захисту інформації України. *Звіт про стан кібербезпеки*. Київ, 2022. 101 с.
7. Human Rights Watch. World Report 2022: Cybersecurity and Human Rights. New York, 2022. 88 p.

Антонюк Антоніна Геннадіївна — студентка групи БМ-23б, факультет будівництва, цивільної та екологічної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: antoniukantonina@gmail.com

Науковий керівник: **Корнієнко Валерій Олександрович** – доктор політичних наук, професор, завідувач кафедри соціально-політичних наук, Вінницький національний технічний університет, м. Вінниця, e-mail: valkorney1958@gmail.com

Antoniuk Antonina H. - student of group BM-23b, Faculty of Construction, Civil and Environmental Engineering, Vinnytsia National Technical University, Vinnytsia, email: antoniukantonina@gmail.com

Supervisor: **Kornienko Valerii** – Dr. of Political Sciences, Professor, Head of the Department of Social and Political Sciences, Vinnytsia National Technical University, Vinnitsa, e-mail: valkorney1958@gmail.com