DOI: https://doi.org/10.71404/PPSS.2023.1.146

КІБЕРСТІЙКІСТЬ ЦИФРОВОЇ ДЕРЖАВИ ЯК ГАРАНТІЯ БЕЗПЕРЕРВНОСТІ ПУБЛІЧНИХ ФУНКЦІЙ

Юрій Олександрович ВИХОДЕЦЬ,

доктор філософії, доцент, професор кафедри
кримінології та інформаційних технологій
Національної академія внутрішніх справ

Цифрова держава створює нову якість публічного управління, однак водночас формує новий профіль правових і безпекових викликів. Якщо раніше інформаційна безпека переважно пов'язувалася із захистом інформації, інформаційних ресурсів і технічних систем, то в умовах цифрової держави об'єктом правового забезпечення стає не лише інформація як така, а й здатність публічної влади безперервно виконувати свої функції у цифровому середовищі.

Актуальність теми посилюється тим, що державні функції, адміністративні процедури, електронні послуги, публічні реєстри, електронна ідентифікація та міжвідомча взаємодія дедалі більше залежать від стабільності цифрової інфраструктури, достовірності даних, доступності сервісів і довіри громадян до цифрових механізмів держави. У разі порушення роботи таких систем виникає не лише технічний інцидент, а й правова проблема: можуть бути порушені права людини, ускладнено доступ до публічних послуг, поставлено під сумнів достовірність реєстрових даних, заблоковано адміністративні процедури або знижено довіру до державних рішень. Для України це питання має особливу значущість у зв'язку з воєнними загрозами, системними кібератаками, інформаційними операціями, ризиками порушення роботи державних цифрових сервісів та євроінтеграційним напрямом розвитку законодавства. Європейський підхід, відображений, зокрема, у NIS2 Directive та Interoperable Europe Act, демонструє перехід від вузького захисту окремих систем до забезпечення високого рівня кібербезпеки, інтероперабельності та стійкості публічного сектору [1; 2].

Класична модель інформаційної безпеки, орієнтована переважно на охорону інформації, інформаційних систем і каналів зв'язку, є необхідною, але вже недостатньою для цифрової держави. У цифровому середовищі кібератака або технічний збій можуть впливати не лише на конфіденційність, цілісність чи доступність інформації, а й на здатність держави реалізовувати публічні функції. Проблема полягає у потребі правового переходу від моделі «захисту систем» до моделі «забезпечення функціональної стійкості».

Метою дослідження є обґрунтування необхідності переходу від традиційного розуміння інформаційної безпеки як захисту інформації та систем до ширшої правової моделі кіберстійкості цифрової держави, спрямованої на забезпечення безперервності публічних функцій, прав людини і довіри до цифрового середовища.

Питання інформаційної безпеки, кібербезпеки та правового забезпечення цифрового середовища досліджувалися у працях українських і зарубіжних учених. В.Г. Пилипчук, В.М. Брижко, І.М. Доронін та інші автори розглядали взаємозв'язок прав людини, приватності та безпеки в інформаційну епоху [3]. О.А. Баранов акцентував увагу на необхідності коректного визначення об'єкта і предмета правового регулювання інтернет-відносин [4]. Г.В. Форос та В.С. Жогов аналізували особливості трактування поняття кібербезпеки в сучасній юридичній науці [5]. У зарубіжній доктрині важливе значення мають підходи Л. Лессіга щодо регулятивної ролі цифрової архітектури [6], а також дослідження М. Бовенса та С. Зурідіса про трансформацію адміністративної дискреції в умовах інформаційно-комунікаційних технологій [7].

Ці підходи дозволяють розглядати цифрову державу не лише як систему технологічних інструментів, а як середовище юридично значимих процедур, у якому архітектура цифрових систем може впливати на межі реалізації прав і повноважень. Водночас у науковій літературі потребує подальшого розвитку саме правове розуміння кіберстійкості цифрової держави як категорії, що виходить за межі технічного кіберзахисту і пов'язана з безперервністю публічних функцій, правовою визначеністю, відновлюваністю, відповідальністю та підтриманням довіри громадян.

Цифрова держава є складною соціотехнічною та правовою системою, у якій публічна влада реалізується через цифрове середовище. У такій моделі інформаційні системи, електронні реєстри, цифрові сервіси, електронна ідентифікація, цифрові документи та канали міжвідомчої взаємодії набувають не лише технічного, а й юридичного значення. Вони стають умовою реалізації прав людини, виконання адміністративних процедур, підтвердження юридично значимих фактів і функціонування органів публічної влади.

У цьому контексті інформаційна безпека зберігає фундаментальне значення, однак її традиційне розуміння має бути доповнене категорією кіберстійкості. Кібербезпека передусім спрямована на запобігання, виявлення, припинення та мінімізацію кіберзагроз. Кіберстійкість, натомість, орієнтована на здатність цифрової держави функціонувати, адаптуватися і відновлюватися в умовах реалізованої кібератаки, технічного збою або іншого порушення нормального функціонування цифрового середовища.

Правова сутність кіберстійкості полягає у тому, що держава повинна не лише захищати інформаційні системи, а й гарантувати безперервність критичних цифрових функцій, юридичну визначеність цифрових процедур, збереження правового значення даних, доступ особи до публічних послуг, можливість відновлення порушених процесів і відповідальність суб'єктів за неналежне функціонування цифрових механізмів.

Тому інформаційна система в цифровій державі має розглядатися не як кінцевий об'єкт охорони, а як засіб реалізації прав, свобод і законних інтересів людини, суспільства та держави. Якщо кібератака призводить до втрати доступу до реєстру, неможливості отримати адміністративну послугу, порушення цілісності даних або блокування цифрової ідентифікації, то наслідки такого інциденту виходять за межі технічної площини. Вони набувають адміністративно-правового, інформаційно-правового, безпекового і правозахисного значення.

У цьому полягає принципова відмінність між охоронною та стійкісною моделями. Охоронна модель відповідає на питання: як запобігти порушенню інформаційної системи? Стійкісна модель відповідає на ширше питання: як забезпечити продовження або відновлення публічної функції, якщо порушення вже відбулося? Саме друга модель є більш придатною для цифрової держави, оскільки абсолютне запобігання всім кіберінцидентам є нереалістичним, тоді як правова спроможність держави діяти в умовах інциденту є необхідною умовою довіри до цифрового публічного управління.

Кіберстійкість цифрової держави має щонайменше три взаємопов'язані виміри. Перший – функціональний: держава повинна забезпечувати безперервність або оперативне відновлення критичних цифрових сервісів. Другий – правовий: цифрові процедури, дані та рішення мають зберігати юридичну визначеність, а особа повинна мати механізми захисту своїх прав. Третій – інституційний: мають бути визначені компетенція суб'єктів, порядок реагування, міжвідомча взаємодія, відповідальність і контроль.

Наукова значущість запропонованого підходу полягає у зміщенні акценту з технічного захисту систем до правового забезпечення функціональної спроможності цифрової держави. Це дозволяє розглядати інформаційну безпеку і кіберстійкість не як ізольовані напрями, а як взаємопов'язані умови стабільності цифрового публічного управління, захисту прав людини та довіри до держави.

Таким чином, можна зробити такі висновки:

1. Інформаційна безпека у цифровій державі не може обмежуватися охороною інформації, інформаційних систем і технічних каналів зв'язку. Вона має бути доповнена правовою моделлю кіберстійкості, спрямованою на забезпечення безперервності публічних функцій.

2. Кіберстійкість цифрової держави доцільно розуміти як юридично врегульовану, організаційно забезпечену та технологічно підтриману здатність держави запобігати кіберзагрозам, витримувати кіберінциденти, підтримувати або відновлювати критичні цифрові функції та гарантувати захист прав людини.

3. Практичне значення кіберстійкості полягає у тому, що кожна державна цифрова система має оцінюватися не лише за показниками функціональності та захищеності, а й за здатністю забезпечувати правову визначеність, відновлюваність, відповідальність і довіру в умовах кіберкризи.

Список використаних джерел:

1. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

2. Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act). URL: https://eur-lex.europa.eu/eli/reg/2024/903/oj.

3. Захист прав, приватності та безпеки людини в інформаційну епоху : монографія / В. Г. Пилипчук, В. М. Брижко, І. М. Доронін та ін. ; за заг. ред. В. Г. Пилипчука. Київ ; Одеса : Фенікс, 2020. 260 с.

4. Баранов О. А. Інтернет і право: об'єкт і предмет регулювання. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*. 2011. № 4. С. 155-162.

5. Форос Г. В., Жогов В. С. Особливості трактування поняття «кібербезпека» в сучасній юридичній науці. *Правова держава*. 2019. № 33. С. 128–134.

6. Lessig L. Code and Other Laws of Cyberspace. Version 2.0. New York : Basic Books, 2006. 432 p.

7. Bovens M., Zouridis S. From Street-Level to System-Level Bureaucracies: How Information and Communication Technology is Transforming Administrative Discretion and Constitutional Control. *Public Administration Review*. 2002. Vol. 62, Issue 2. P. 174-184.