DOI 10.34132/mspc2025.01.11.01

Ірина Бердиченко

ПЕРСПЕКТИВИ ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Тези представляють теоретико-методологічний аналіз питання удосконалення нормативно-правової бази у сфері кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури, як важливого чинника у розбудові ефективного захисту від кібератак інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси.

Наголошується, що діяльність з побудови ефективної нормативно-правової бази з метою посилення спроможностей з кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури не може бути статичною, така діяльність повинна продовжуватися і надалі, з урахуванням нових ризиків, які виникають у сфері функціонування державних інформаційних ресурсів та критичної інформаційної інфраструктури, та з метою впровадження найкращих європейських практик.

Ключові слова: *кіберзахит, державні інформаційні ресурси, об'єкти критичної інформаційної інфраструктури, Європейський Союз.*

Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, яка діє при Держспецзв'язку, у 2024 році опрацювала 4315 кіберінцидентів. Це на 69,8% більше, ніж роком раніше, коли кіберзлочинці атакували український кіберпростір 2541 раз. Найчастіше зловмисники атакують місцеві органи влади, уряд та урядові організації, сектор безпеки та оборони та енергетичний сектор. Існує стійка тенденція збільшення кількості загроз національній безпеці у кіберпросторі. Якщо у першому півріччі минулого року на урядові організації було здійснено 473 кібератаки, то у другому вже було зафіксовано 665 випадків (+41%). Зросла минулого року і кількість кібератак на місцеві органи влади: від 542 випадків у першому півріччі до 831 у другому (+53%). На 82% збільшилася кількість кібератак на сектор безпеки і оборони: 276 інцидентів у першому півріччі та 502 – у другому [1]. Численні кібератаки мають на меті підрив національної безпеки України, насамперед, шляхом заподіяння шкоди державним інформаційним ресурсам та об'єктам критичної інформаційної інфраструктури. Вищеназвані чинники, свідчать про необхідність подальшої роботи над удосконаленням національного законодавства у сфері кібербезпеки, що є необхідним для мінімізації загроз кібербезпеці України, і перш за все щодо захищеності від кібератак державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури.

Відповідно до частини першої статті 1 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» [2] державні інформаційні ресурси це систематизована інформація, що є доступною за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить державним органам, військовим формуванням, утвореним відповідно до законів України, державним підприємствам, установам та організаціям, а також інформація, створення якої передбачено законодавством та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень.

Наразі актуальним є системна робота з підвищення кіберстійкості в умовах зростаючих кіберзагроз, посилення готовності державних органів до реагування на інциденти будь-якого рівня складності, робота над законодавчими змінам у сфері кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури, розвиток стратегічного реагування на кіберінциденти у державних інформаційних ресурсах та удосконалення міжвідомчій взаємодії у цих сферах.

Нормативно-правовою базою в сфері правового регулювання кіберзахисту державних інформаційних ресурсів, є:

– Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» (Відомості Верховної Ради України (ВВР), 2014 р., № 25, ст. 890 із змінами);

– Закон України «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403 із змінами) [3];

– Закон України «Про захист інформації в інформаційно-комунікаційних системах» (Відомості Верховної Ради України (ВВР), 1994, № 31, ст.286 із змінами) [4];

– Закон України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності» (Відомості Верховної Ради України (ВВР), 2007, № 29, ст.389 із змінами) [5];

– Закон України «Про функціонування паливно-енергетичного комплексу в особливий період» (Відомості Верховної Ради України, 2006 р., № 52, ст. 526 із змінами) [6];

– Закон України «Про національну безпеку України» (Відомості Верховної Ради України, 2018 р., № 31, ст. 241 із змінами) [7];

– Закон України «Про стандартизацію» (Відомості Верховної Ради (ВВР), 2014, № 31, ст.1058 із змінами) [8].

Наразі актуальним для національного законодавства, у тому числі у сфері кібербезпеки та кіберзахисту, є адаптація законодавства України до законодавства Європейського Союзу насамперед до Директиви (ЄС) 2022/2555 Європейського Парламенту і Ради від 14.12.2022 про заходи щодо забезпечення високого загального рівня кібербезпеки у всьому Союзі, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972, а також скасування Директиви (ЄС) 2016/1148) (NIS 2) [9].

Також перспективним та корисним є унормування використання стандартів, настанов, рекомендацій, аналітичних оглядів та інших документів, розроблених та прийнятих іноземними та міжнародними організаціями з питань кіберзахисту, у тому числі документів Міжнародної організації зі стандартизації (ISO), Європейського комітету зі стандартизації (CEN), Європейського інституту телекомунікаційних стандартів (ETSI), Міжнародного союзу електрозв'язку (ITU), Агентства Європейського Союзу з кібербезпеки (ENISA), Агентства з кібербезпеки та безпеки інфраструктури (CISA), Національного інституту стандартів та технологій (NIST), Організації Північноатлантичного договору (NATO), а також визнаних зазначеними організаціями процедур оцінки відповідності, у тому числі сертифікації, рекомендованої для застосування у сферах організації спеціального зв'язку, криптографічного та технічного захисту інформації, кіберзахисту.

Стратегія кібербезпеки як документ, що визначає пріоритети, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, повинна формуватися та уточнюватися з урахуванням положень європейського законодавства у сфері кібербезпеки, у тому числі з урахуванням положень Директиви Європейського Союзу щодо мережевої та інформаційної безпеки (NIS 2).

Водночас, важливим напрямком є впорядкування на рівні Закону створення та забезпечення функціонування національних систем реагування на інциденти кібербезпеки, кібератаки, кіберзагрози та обміну інформацією про інциденти кібербезпеки щодо інформаційних, електронних комунікаційних інформаційно-комунікаційних та технологічних систем, в яких оброблюються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом; розбудова в рамках національної системи реагування команд реагування та визначення ролей і завдань національної, галузевих та регіональних команд реагування з урахуванням рекомендацій, визначених NIS 2.

Крім зазначених питань щодо євроінтеграційних процесів, слід наголосити на необхідності подальших кроків з удосконалення законодавства за такими напрямками як:

- розбудова профільних підрозділів з кіберзахисту в державних органах, на об'єктах критичної інфраструктури, а також визначення типових вимог до таких підрозділів та їх керівників;
- удосконалення взаємодії суб'єктів реагування у разі настання кризової ситуації в кібербезпеці;
- впровадження комплексного підходу до організації навчань, тренінгів з кіберзахисту та захисту інформації, а також інструктажів з кібергігієни.

Робота за цими напрямками упорядкування законодавства у сфері кібербезпеки та кіберзахисту є вкрай важливою та необхідною, водночас потребує виваженого підходу та врахування принципів законності, юридичної визначеності, запобігання зловживанню повноваженнями.

Звернемо увагу на деякі питання удосконалення законодавства за вищезгаданими напрямками, які викликають дискусії та застереження. Активну роль серед профільних підрозділів у сфері кібербезпеки відіграє Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України (далі – РНБО).

Відповідно до частини першої та другої статті 5 Закону України «Про основні засади забезпечення кібербезпеки України» координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України.

Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та загальний контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, загальну координацію суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози; подає до Ради національної безпеки і оборони України пропозиції щодо оголошення кризової ситуації в кібербезпеці; координує реалізацію Стратегії кібербезпеки України, подає до Ради національної безпеки і оборони України пропозиції щодо формування та уточнення Стратегії, у тому числі з урахуванням положень Директиви Європейського Союзу щодо мережевої та інформаційної безпеки (NIS 2); визначає пріоритети, розробляє концептуальні засади та вносить Президентові України пропозиції щодо проведення кібероперацій стратегічного рівня в інтересах національної безпеки і оборони та забезпечує координацію суб'єктів сектору безпеки і оборони щодо їх проведення; координує стратегічні комунікації у сфері кібербезпеки.

Вклад спеціалістів вказаного центру у діяльність з кіберзахисту національного кіберпростору не викликає сумнівів, а лише повагу. Проте, при роботі над законодавчим визначенням особливостей правового статусу цього органу, як і інших робочих органів РНБО необхідно пам'ятати про конституційну модель організації влади в державі, яка базується на положеннях статті 6 Конституції України, згідно з якою державна влада в Україні здійснюється на засадах її поділу на законодавчу, виконавчу та судову. Відповідно до рішення Конституційного Суду України від 16 вересня 2020 року № 11-р/2020 [10]: «конституційний припис щодо поділу влади на законодавчу, виконавчу та судову як один із фундаментальних приписів щодо здійснення державної влади неодноразово розглядався Конституційним Судом України не тільки як такий, що покликаний відображати функційну визначеність кожного з державних органів (місце в системі стримувань і противаг) та забезпечувати самостійне виконання державними органами своїх функцій і повноважень, а й утверджувати права і свободи людини і громадянина та забезпечувати стабільність конституційного ладу в державі. Зазначений конституційний припис є субстанційною ознакою правової держави, тому недотримання принципу поділу влади загрожує виконанню державою покладених на неї Основним Законом України обов'язків, особливо передбачених частиною другою статті 3 Конституції України». Крім того, згідно з частиною другою статті 14 Закону України «Про Раду національної безпеки і оборони України» [11] функції та повноваження робочих та консультативних органів РНБО визначаються окремими положеннями, які затверджує Президент України.

Продовжуючи тематику розбудови профільних підрозділів у сфері кібезбезпеки та кіберзахисту та забезпеченні контролю за призначенням керівників таких підрозділів у державних органах необхідно оцінити ризики та передбачити застереження втручання контролюючих органів і можливість їх впливу на кадрову політику в інших органах державної влади діяльність яких регулюється їхніми базовими законами, насамперед Закон України «Про центральні органи виконавчої влади», а також дотримання принципу правової визначеності (стаття 8 Конституції України).

Крім того, необхідно враховувати положення профільних Законів в частині організації керівництва відповідними органами державної влади та органами місцевого самоврядування, передбачених базовими законами, якими регулюється діяльність зазначених органів, наприклад, пункт 1 частини першої статті 42 Закону України «Про Кабінет Міністрів України» [12], пункт 1 частини другої статті 8, пункт 1 частини четвертої статті 19 Закону України «Про центральні органи виконавчої влади» [13], пункт 2 частини шостої статті 15 Закону України «Про правовий режим воєнного стану» [14].

Україна щоденно стикається з реальністю постійно зростаючої кількості кібератак та динамічного ландшафту загроз. З огляду на зазначене, залишається актуальним врегулювання нових механізмів захисту державних інформаційних ресурсів та критичної інформаційної інфраструктури, упорядковування координації у сфері кібербезпеки та наближення національного законодавства до європейських практик та стандартів, подальший розвиток державно-приватного партнерства, співпраці з міжнародними партнерами, що дозволить підвищити ефективність інтеграції у глобальну систему кіберзахисту, і відповідно, підвищити стійкість національної цифрової екосистеми до сучасних викликів.

References

1. CERT-UA mynuloho roku opratsiuvala 4315 kiberintsydentiv (onlain) URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv.
2. Zakon Ukrainy «Pro Derzhavnu sluzhbu spetsialnoho zviazku ta zakhystu informatsii Ukrainy» (Vidomosti Verkhovnoi Rady Ukrainy (VVR), 2014 r., № 25, st. 890 iz zminamy) (onlain) URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text.
3. Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» (Vidomosti Verkhovnoi Rady (VVR), 2017, № 45, st.403 iz zminamy) (onlain) URL: https://zakon.rada.gov.ua/laws/show/2163-19.
4. Zakon Ukrainy «Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh» (Vidomosti Verkhovnoi Rady Ukrainy (VVR), 1994, № 31, st.286 iz zminamy) (onlain) URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
5. Zakon Ukrainy «Pro osnovni zasady derzhavnoho nahliadu (kontroliu) u sferi hospodarskoi diialnosti» (Vidomosti Verkhovnoi Rady Ukrainy (VVR), 2007, № 29, st.389 iz zminamy) (onlain) URL: https://zakon.rada.gov.ua/laws/show/877-16#Text.
6. Zakon Ukrainy «Pro funktsionuvannia palyvno-enerhetychnoho kompleksu v osoblyvyi period» (Vidomosti Verkhovnoi Rady Ukrainy, 2006 r., № 52, st. 526 iz zminamy) (onlain) URL: https://zakon.rada.gov.ua/laws/show/307-16#Text.
7. Zakon Ukrainy «Pro natsionalnu bezpeku Ukrainy» (Vidomosti Verkhovnoi Rady Ukrainy, 2018 r., № 31, st. 241 iz zminamy) (onlain) URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.
8. Zakon Ukrainy «Pro standartyzatsiiu» (Vidomosti Verkhovnoi Rady (VVR), 2014, № 31, st.1058 iz zminamy) (onlain) URL: https://zakon.rada.gov.ua/laws/show/1315-18#Text.
9. Dyrektyva (YeS) 2022/2555 Yevropeiskoho Parlamentu i Rady vid 14.12.2022 pro zakhody shchodo zabezpechennia vysokoho zahalnoho rivnia kiberbezpeky u vsomu Soiuzi, vnesennia zmin do Rehlamentu (YeS) № 910/2014 ta Dyrektyvy (YeS) 2018/1972, a takozh skasuvannia Dyrektyvy (YeS) 2016/1148) (onlain) URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.
10. Rishennia Konstytutsiinoho Sudu Ukrainy vid 16 veresnia 2020 roku № 11-r/2020 (onlain) URL: https://zakon.rada.gov.ua/laws/show/v011p710-20#Text.

11. Zakon Ukrainy «Pro Radu natsionalnoi bezpeky i oborony Ukrainy» (Vidomosti Verkhovnoi Rady Ukrainy (VVR), 1998, № 35, st. 237) (onlain) URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text.
12. Zakon Ukrainy «Pro Kabinet Ministriv Ukrainy» (Vidomosti Verkhovnoi Rady (VVR), 2014, № 13, st.222) (onlain) URL: https://zakon.rada.gov.ua/laws/show/794-18#Text.
13. Zakon Ukrainy «Pro tsentralni orhany vykonavchoi vlady» (Vidomosti Verkhovnoi Rady Ukrainy (VVR), 2011, № 38, st.385) (onlain) URL: https://zakon.rada.gov.ua/laws/show/3166-17#Text.
14. Zakon Ukrainy «Pro pravovyi rezhym voiennoho stanu» (Vidomosti Verkhovnoi Rady (VVR), 2015, № 28, st.250) (onlain) URL: https://zakon.rada.gov.ua/laws/show/389-19#Text.

DOI 10.34132/mspc2025.01.11.01

Iryna Berdychenko

PROSPECTS OF LEGAL REGULATION OF CYBER PROTECTION OF STATE INFORMATION RESOURCES

The theses present a theoretical and methodological analysis of the issue of improving the regulatory framework in the field of cybersecurity regarding cyber protection of state information resources and critical information infrastructure, as an important factor in developing effective protection against cyber attacks of information, electronic communication and information and communication systems in which state information resources are processed.

It is emphasized that activities to build an effective regulatory framework to strengthen cyber protection capabilities of state information resources and critical information infrastructure cannot be static; such activities must continue in the future, taking into account new risks that arise in the field of functioning of state information resources and critical information infrastructure and in order to implement best European practices.

Key words: *cyber defense, state information resources, critical information infrastructure facilities, European Union.*

Відомості про автора / Information about the Author

Ірина Бердиченко, канд. юрид. наук, професор Міжнародної Кадрової Академії, старший викладач кафедри цивільного та кримінального права і процесу, Чорноморського національного університету імені Петра Могили, м. Миколаїв, Україна. E-mail: gsu_546@ukr.net, orcid: https://orcid.org/0000-0002-6670-433X.

Iryna Berdychenko, candidate of legal sciences, Professor of the International Personnel Academy, Senior Lecturer, Department of Civil and Criminal Law and Procedure, Petro Mohyla Black Sea National University, Mykolaiv, Ukraine. E-mail: gsu_546@ukr.net, orcid: https://orcid.org/0000-0002-6670-433X.

Стаття отримана редакцією 22.05.2025.