ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 34(63). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 34(63). Category «B»
https://doi.org/10.58442/3041-1858-2025-34(63)

https://doi.org/10.58442/3041-1858-2025-34(63)-236-252
УДК 346

Корягін Артем Володимирович,
аспірант кафедри публічного управління і проектного менеджменту
Навчально-наукового інституту менеджменту та психології
ДЗВО «Університет менеджменту освіти».
Київ, Україна.
a_koryagin@ukr.net

ПЕРІОДИЗАЦІЯ СТАНОВЛЕННЯ ТА РОЗВИТКУ ОРГАНІЗАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЕНЕРГЕТИЧНІЙ СФЕРІ В УКРАЇНІ

Анотація. У публікації наведено результатами дослідження щодо попереднього аналізу сучасного стану проблемних питань організаційно-правового забезпечення інформаційної безпеки в енергетичній сфері. Окреслено періодизацію становлення та розвитку організаційно-правового забезпечення інформаційної безпеки в енергетичній сфері в Україні на основі значимих правових подій. За зібраними даними проаналізовано тенденції розвитку організаційно-правового забезпечення інформаційної безпеки в енергетичній сфері в Україні як об'єкта публічного регуляторного впливу. Виявлено значимі правові події, визначено особливості та дієві фактори за періодами. Військова агресія Російської Федерації стала додатковим каталізатором змін та управлінських дій у цій сфері, внаслідок реалізації нових нормативно-правових актів України, обумовлених цією агресією. Майбутній розвиток організаційно-правового забезпечення інформаційної безпеки в енергетичній сфері в Україні пов'язаний із інтеграцією з міжнародними стандартами (міжнародні стандарти ISO/IEC у сфері інформаційної безпеки, європейська директива NIS2 Directive). Представлені результати досліджень є початковою ланкою в обґрунтування теоретико-методологічних засад організаційно-правових механізмів та інструментів забезпечення інформаційної безпеки в енергетичній сфері в Україні.

Ключові слова: інформаційна безпека; організаційно-правове забезпечення; публічне регулювання; кіберпростір та кібербезпека.

ВСТУП / INTRODUCTION

Постановка проблеми / Statement of the problem. Реалії сьогодення переконливо свідчать суб'єктам системи публічного управління, що

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 34(63). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 34(63). Category «B»
https://doi.org/10.58442/3041-1858-2025-34(63)

забезпечення національної безпеки України та її складової – інформаційної безпеки України, є факторами як виживання, стійкості в умовах збройної агресії проти країни, так й відновлення, економічного і соціального розвитку країни. Особливо нагальним та важливим є забезпечення дієвого захисту критичної інфраструктури паливно-енергетичного комплексу в енергетичній сфері від зловмисних дій груп осіб, а також від техногенно-екологічних впливів.

Аналіз термінології нормативно-правового забезпечення та науково-категорійного апарату свідчить про розподіл в останні роки поняття «інформаційна безпека» (до якої в Україні віднесено негативні інформаційні впливи, розповсюдження та використанні інформації з обмеженим доступом) та окремо питань кібернетичного захисту інформації (технічного та криптографічного захистів). Враховуючи стратегічне значення об'єктів енергетичної сфери в Україні, доцільним вбачається вивчення та вдосконалення питань охорони інформації та захисту інформаційно-телекомунікаційних систем як комплексного підходу та впливу органів системи публічного управління, обґрунтування теоретико-методологічних засад організаційно-правових механізмів та інструментів забезпечення інформаційної безпеки в енергетичній сфері і розробка практичних рекомендацій органам публічної влади щодо його вдосконалення в Україні.

Для аналізу сфери досліджуваних відносин, доцільно встановити періодизацію становлення та розвитку публічного регулювання забезпечення інформаційної безпеки в енергетичній сфері в Україні. Це дозволить виокремити якісно відмінні етапи розвитку суспільних процесів за критеріями зміни нормативно-правової бази, інституційного середовища та рівня інтеграції у міжнародні стандарти.

Аналіз (основних) останніх досліджень і публікацій / Analysis of (major) recent research and publications. У науковій літературі напрямок наукових досліджень публічного регулювання діяльності щодо організаційно-правового забезпечення інформаційної безпеки в України є достатньо досліджений за різними аспектами. Водночас, внаслідок впливу суспільних процесів та періодичних змін векторів щодо організації та методологічних підходів у розбудові системи інформаційної безпеки Україна як держава отримала Доктрину інформаційної безпеки лише у 2009 році, а з 2016 року відбулось перезавантаження та розвиток одночасно двох напрямків стратегічного планування та розвитку організаційно-правового забезпечення – як «інформаційної безпеки» в аспекті деструктивних

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 34(63). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 34(63). Category «B»
https://doi.org/10.58442/3041-1858-2025-34(63)

(зловмисних) впливів, а також «кібербезпеки» як її спеціалізованої функціональної сфери інформаційно-телекомунікаційних відносин.

Відповідно до цих загальних тенденцій у цей же час розбудовувались системи інформаційної безпеки на об'єктах енергетичної сфери України.

Питання інформаційної безпеки, кібербезпеки та кіберзахисту досліджувала значна кількість науковців та дослідників: Г. Андрощук, В. Артемов, В. Бутузов, В. Гавловський, С. Гнатюк, В. Домарєв, А. Гуз, А. Марущак, О. Онищенко, Ю. Орлов, В. Хорошко та інші. На рівні дисертації досліджували Ю. Бурило, Б. Кормич, В. Гурковський. Результати досліджень питань інформаційної безпеки у монографіях розкривали В. Антонов, М. Биченок, О. Довгань. Власні дослідження щодо стану та динаміки досліджуваної сфери відносин за останні роки публікували К. Войтовський, С. Демедюк, А. Лепіхо, В. Лук'яненко, І. Паливода, О. Резнікова та інші.

Незважаючи на значне коло наукових напрацювань щодо державного регулювання в різних сферах життєдіяльності суспільства, теоретико-методологічні засади організаційно-правових механізмів та інструментів забезпечення інформаційної безпеки в енергетичній сфері ще не сформовано належним чином.

МЕТА ТА ЗАВДАННЯ / AIM AND TASKS

Мета статті полягає у теоретичному аналізі та визначенні основних етапів формування організаційно-правового забезпечення інформаційної безпеки в енергетичній сфері.

Відповідно до зазначеної мети у статті поставлено такі ***завдання***: установити періодизацію становлення та розвитку організаційно-правового забезпечення інформаційної безпеки в енергетичній сфері на основі значимих правових подій; проаналізувати тенденції розвитку стану інформаційної безпеки в енергетичній сфері як об'єкта публічного регуляторного впливу.

ТЕОРЕТИЧНІ ОСНОВИ / THEORETICAL FRAMEWORK

Визначальними для періодизації становлення та розвитку організаційно-правового забезпечення інформаційної безпеки в енергетичній сфері в Україні стали такі значимі правові події:

- 1992 рік – прийняття Закону України «Про інформацію» (№ 2657-XII, чинний);
- 1994 рік – прийняття Закону України «Про захист інформації в інформаційно-комунікаційних системах» (на дату прийняття мав іншу

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 34(63). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 34(63). Category «B»
https://doi.org/10.58442/3041-1858-2025-34(63)

назву – «Про захист інформації в автоматизованих системах», № 80/94-ВР, чинний);

- 1996 рік – прийняття Конституції – Основного Закону України) (№ 254к/96-ВР, чинний);
- 2003 рік – прийняття Закону України «Про основи національної безпеки» (№ 964-IV, втратив чинність 08 липня 2018 року);
- 2005 рік – прийняття Закону України «Про ратифікацію Конвенції про кіберзлочинність» (№ 2824-IV, чинний);
- 2009 рік – затвердження першої Доктрини інформаційної безпеки України Указом Президента (№ 514/2009, втратила чинність 06 червня 2014 року);
- 2016 рік – затвердження першої Стратегії кібербезпеки України Указом Президента (№ 96/2016, втратила чинність 26 серпня 2021 року);
- 2017 рік – затвердження другої Доктрини інформаційної безпеки України Указом Президента (№ 47/2017, втратила чинність 28 грудня 2021 року);
- 2021 рік – затвердження оновленої Стратегії кібербезпеки України Указом Президента (№ 447/2021, чинний);
- 2021 рік – прийняття Закону України «Про критичну інфраструктуру» (№ 1882-IX, чинний);
- 2021 рік – затвердження Стратегії інформаційної безпеки України Указом Президента (№ 685/2021, чинний).

Відповідно до правових подій в Україні можемо визначити 5 етапів, коли відбувалося прийняття системних, профільних нормативно-правових актів, які законодавчо врегулювали питання інформаційної безпеки, у тому числі в енергетичній сфері:

1. Початковий етап формування правових засад: 1991–2000 роки.

Перший етап характеризується:

- визначенням загальних засад державної політики у сфері інформаційної безпеки та енергетики;
- прийняття Конституції України, яка визначила засади національної безпеки та інформаційної безпеки.

Згідно абзацу 1 статті 17 Конституції України, «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу».

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 34(63). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 34(63). Category «B»
https://doi.org/10.58442/3041-1858-2025-34(63)

У чинному Законі «Про інформацію» визначено термін «захист інформації» – це сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

У чинному Законі «Про захист інформації в інформаційно-комунікаційних системах» визначені терміни: «захист інформації в системі» – діяльність, спрямована на запобігання порушенню цілісності, конфіденційності і доступності інформації в системі; «комплексна система захисту інформації» – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації; «криптографічний захист інформації» – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо; «технічний захист інформації» – вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

2. Етап інституціоналізації та нормативно-правового оформлення: 2001–2013 роки.

Другий етап характеризується:

- прийняття Закону України «Про основи національної безпеки України» (згодом втратив чинність з 2018 року);
- становлення та розвиток державних інституцій, до компетенції яких віднесені питання забезпечення інформаційної безпеки: РНБО України, Держспецзв’язку;
- затвердження першої Доктрини інформаційної безпеки України Указом Президента (згодом втратила чинність 06 червня 2014 року);
- на регіональному та місцевих рівнях власниками підприємств та установ в енергетичній сфері приділяється увага захисту критичної інфраструктури, у тому числі організаційно-правовому забезпеченню інформаційної безпеки в цій сфері.

У Законі України «Про основи національної безпеки України» термін «національна безпека» був визначений як захищеність життєвоважливих інтересів людини і громадянина, суспільства і держави, – із наступним перерахуванням видів загроз та сфер охоронюваних відносин, зокрема: забезпечення свободи слова та інформаційної безпеки, кібербезпеки та

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 34(63). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 34(63). Category «B»
https://doi.org/10.58442/3041-1858-2025-34(63)

кіберзахисту, захисту інформації, інформаційних технологій, енергетики та енергозбереження тощо.

На другому етапі активно досліджувались питання забезпечення інформаційної безпеки, боротьби з комп'ютерною злочинністю та організаційно-правові забезпечення протидії несанкціонованому доступу як різновиду суспільно небезпечних діянь в інформаційній сфері.

Дослідниками надано визначення правової категорії «несанкціонованому доступу до інформаційно-телекомунікаційних систем» – це сукупність різних за характером суспільної небезпеки, але єдиних за своєю суттю діянь (кримінальних, адміністративних, цивільно-правових, господарсько-правових, дисциплінарних) з питань володіння, користування, розпорядження та захисту інформації (яка зберігається, обробляється та передається за допомогою інформаційно-телекомунікаційних систем, а охорона прав та законних інтересів відносно якої передбачена законодавством України), визначених у відповідних статтях кодексів та законів України, підзаконних нормативно-правових актах, а також в угодах між суб'єктами господарювання, трудовими колективами та окремими працівниками [1, с. 244]. Окремо протиправний несанкціонований доступ характеризувався як кримінально-правова категорія.

У правозастосуванні з лютого 2005 року набули чинності нові 6 статей Кримінального кодексу України щодо протидії комп'ютерним злочинам (Розділ XVI кодексу), фактично імплементовано норми матеріального права Конвенції про кіберзлочинність, підписаної Україною у 2001 році. У рамках законопроекту «Про моніторинг телекомунікацій» опрацьовувались питання імплементації норм процесуального права цієї Конвенції.

На цьому етапі з питань концептуального формування політики щодо забезпечення інформаційної безпеки, розроблення та впровадження відповідного організаційно-правового забезпечення на доктринальному рівні Україна поступалася у строках та темпах Росії, Республіці Казахстан, не беручи до уваги питання захисту національних інтересів у розвинених країнах Заходу, як-то Сполучені Штати Америки у Національній стратегії захисту кіберпростору (прийнята у 2003 році).

На другому етапі однією з провідних установ, які забезпечували роботу Апарату РНБО України з питань інформаційної безпеки, розроблення проекту першої Доктрини інформаційної безпеки України (чинна у 2009–2014 роки) був Інститут проблем національної безпеки. Навесні 2010 року цей інститут, а також Національний інститут проблем міжнародної безпеки, були фактично ліквідовані, а весь обсяг їх

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 34(63). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 34(63). Category «B»
https://doi.org/10.58442/3041-1858-2025-34(63)

компетенцій фактично передано до Національного інституту стратегічних досліджень, який серед цих трьох установ спеціалізувався на питаннях економіки, соціології, політології. Причини такого об'єднання науково-дослідних установ, вірогідно, були обумовлені різними векторами напрямків досліджень (європейський та євроатлантичний у Національному інституті проблем міжнародної безпеки), а у випадку Інституту проблем національної безпеки, – ще й фактор міжрегіональних кланових протистоянь у країні, який діяв в цей період.

Одним із наслідків стало, що на наступному третьому етапі відбулося формування окремо напрямку інформаційної безпеки у контексті протидії зловмисним інформаційним впливам (із залишенням загального терміну «інформаційна безпека»), а окремо – напрямку кібербезпеки та кіберзахисту. У науковій періодиці проводився пошук генезиса, основних термінів сфери інформаційної безпеки, її співвідношення із сферою кібернетичної безпеки (кібербезпекою) у публікаціях представників Національного інституту стратегічних досліджень, які, ймовірно, досліджували ці питання в інтересах наукового забезпечення діяльності РНБО України.

3. Етап викликів та адаптації до міжнародних моделей захисту інтересів в інформаційній сфері: 2014–2017 роки.

Третій етап характеризується:

- Початок гібридної агресії РФ та перші масштабні кібератаки на енергетичний сектор України (кібератаки «BlackEnergy» у грудні 2015 року та «BlackEnergy 2/3» у 2016 році) ;
- Усвідомлення та посилення уваги до енергетики як критичної інфраструктури, потенційно вразливої для кіберзагроз;
- прийняття Закону України «Про основні засади забезпечення кібербезпеки України»;
- формування національної системи кіберзахисту, формування інституційних механізмів співпраці з міжнародними структурами, початок інтеграції з практиками НАТО та ЄС.

Про результаті аналізу експертів у сфері кіберзахисту стосовно кібератак BlackEnergy у 2015 та у 2016 році на критичну інфраструктуру енергозабезпечення в Україні повідомлялось у журналі «Forbes» [2].

У грудні 2016 року у Західній Україні сталися перебої з електропостачанням. Міністерство енергетики підтвердило, що перевіряє інформацію про кібератаку, яка 23 грудня спричинила перебої з електропостачанням у Івано-Франківській області, що обслуговується місцевим енергопостачальником «Прикарпаттяобленерго».

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 34(63). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 34(63). Category «B»
https://doi.org/10.58442/3041-1858-2025-34(63)

Служба безпеки України заявила, що російські спроби порушити роботу енергомережі країни були відбиті.

Шкідливе програмне забезпечення незабаром було пов'язане з відомим хакерським інструментом – BlackEnergy – який раніше використовувався у спробах зламати енергопостачальників по всьому світу, включаючи американські організації.

Шкідливе програмне забезпечення BlackEnergy, яке використовувалося в атаках ще з 2007 року, спочатку вважалося орієнтованим на кібершпигунство. Але у 2014 році хакери оновили набір інструментів, додавши шкідливий код, спрямований на SCADA ICS (на автоматизоване управління промисловим обладнанням), відомий своєю вразливістю набір, що використовується для управління електростанціями та іншою критичною інфраструктурою.

Про зв'язок між BlackEnergy і шкідливим програмним забезпеченням KillDisk вперше повідомила CERT-UA ву листопаді 2015 року, коли новини були атаковані під час місцевих виборів в Україні у 2015 році. Це посилило підозри, що до групи були причетні хакери, спонсоровані Росією.

4. Розвиток вітчизняної системи кібербезпеки та євроінтеграція: 2018–2021 роки.

Четвертий етап характеризується:

- формування та розвиток законодавства про критичну інфраструктуру та її захист;
- визначення енергозабезпечення серед життєвоважливих інтересів при визначенні секторів критичної інфраструктури;
- гармонізація національного законодавства з нормами ЄС;
- формування та розвиток публічно-приватних механізмів взаємодії у сфері кіберзахисту.

Станом на 2021 рік науковцями Національного інституту стратегічних досліджень проаналізовано стан національної системи кібербезпеки [3, с. 84].

Національний координаційний центр кібербезпеки функціонує як робочий орган РНБО України, одним з основних завдань якого є координація та контроль за діяльністю суб’єктів сектору безпеки і оборони, які забезпечують кібербезпеку. Державна служба спеціального зв’язку та захисту інформації України (Держспецзв’язку) як центральний орган виконавчої влади координує діяльність інших суб’єктів забезпечення кібербезпеки щодо кіберзахисту, зокрема у процесах реалізації організаційних, правових інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 34(63). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 34(63). Category «B»
https://doi.org/10.58442/3041-1858-2025-34(63)

запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості та надійності функціонування комунікаційних, технологічних систем. Ця функція реалізується через Державний центр кіберзахисту при Держспецзв'язку [3, с. 84].

Урядова команда реагування на комп'ютерні надзвичайні події України (англ. Computer Emergency Response Team of Ukraine, CERT-UA) серед іншого забезпечує взаємодію з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору, у тому числі з питань збирання та накопичення інформації про кіберзагрози та кіберінциденти й реагування на них [3, с. 85].

5. Етап воєнного стану та посилення стійкості: 2022 рік – дотепер.

П'ятий етап характеризується:

- кібератаки на енергетичні об'єкти у період повномасштабного вторгнення країни-агресора;
- розвиток системи державного управління та публічного регулювання на основі воєнного досвіду;
- практичне застосування Закону України «Про критичну інфраструктуру» (прийнятий у 2021 році, введення в дію з 2022 року);
- подальша інтеграція з європейськими та євроатлантичними структурами у сфері кіберзахисту та кібервійни;
- формування нових підходів до публічно-приватного партнерства у сфері захисту енергетичних компаній.

Згідно пункту 2 абзацу 4 статті 9 «Сектори критичної інфраструктури» Закону України «Про критичну інфраструктуру» енергозабезпечення (у тому числі постачання теплової енергії), – безпосередньо визначено серед життєво важливих функцій та/або послуг, порушення яких призводить до негативних наслідків для національної безпеки України.

У абзаці 2 цієї статті закону визначено, що Перелік секторів критичної інфраструктури та суб'єктів, відповідальних за формування та реалізацію державної політики у відповідних секторах національної системи захисту критичної інфраструктури, визначається Кабінетом Міністрів України.

За період п'ятого етапу є один новий нормативно-правовий акт України загальнодержавного рівня, спрямований на розвиток Стратегії інформаційної безпеки України (затвердженої у 2021 році), – це Розпорядження Кабінету Міністрів України від 30 березня 2023 року № 272-р «Про затвердження плану заходів з реалізації Стратегії інформаційної

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 34(63). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 34(63). Category «B»
https://doi.org/10.58442/3041-1858-2025-34(63)

безпеки на період до 2025 року», відповідальним за звітування по плану визначено Міністерство культури та інформаційної політики.

За іншим напрямом, на розвиток Стратегії кібербезпеки України (затверджена у 2016 році, оновлена у 2021 році) періодично доповнюється нормативно-правове забезпечення загальнодержавного рівня, яке в подальшому формує стратегічний, регіональний та місцевий рівні організаційно-правового забезпечення кібербезпеки та інформаційної безпеки.

Аналіз положень Плану заходів на 2025 рік з реалізації положень Стратегії кібербезпеки України, затвердженого розпорядженням Кабінету Міністрів України від 7 березня 2025 року № 204-р [4], свідчить про сучасні акценти у скеруванні підрозділів Національної поліції, Міністерства внутрішніх справ (МВС) та Служби безпеки України (СБУ). Національна поліція та МВС посилюють технічні можливості, зокрема, згідно пункту 7 Плану індикатором виконання є імплементація в законодавство України положення Конвенції про кіберзлочинність щодо термінового збереження комп'ютерних даних. Згідно пункту 5 Плану СБУ, після погодження, індикатором виконання є проведення запланованих негласних перевірок стану готовності об'єктів критичної інфраструктури до можливих кібератак і кіберінцидентів, зокрема шляхом пошуку та виявлення потенційних вразливостей інформаційно-комунікаційних систем об'єктів критичної інфраструктури.

У перші місяці повномасштабного вторгнення Росії, зі сторони законодавця увага правоохоронців була зосереджена на посиленні кримінальної відповідальності по статті 361 Кримінального кодексу України (має альтернативну підслідність Національної поліції та Служби безпеки України). Законом України від 23 серпня 2023 року № 3342-IX «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» [5] зазначену статтю кодексу доповнено частинами 4 та 5, відповідно.

4. Дії, передбачені частиною першою або другою цієї статті (несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, також вчинені повторно або за попередньою змовою групою осіб), якщо вони заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків, – караються позбавленням волі на строк від восьми до

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 34(63). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 34(63). Category «B»
https://doi.org/10.58442/3041-1858-2025-34(63)

дванадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.

5. Дії передбачені частиною третьою (дії, передбачені частиною першою чи другою статті, якщо вони призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації) та четвертою цієї статті, вчинені під час дії воєнного стану, – караються позбавленням волі на строк від десяти до п’ятнадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

Слід констатувати, що в умовах воєнного стану цей кіберзлочин за статтею 361 Кримінального кодексу України «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж» отримав ступінь особливої тяжкості.

Питання інформаційної безпеки та захисту об’єктів енергетики набувають актуальності й в зарубіжних країнах.

На досвіді Польщі спостерігається науково-практичний інтерес саме до цих питань, кібернетичного захисту критичних об’єктів енергетичної інфраструктури.

Більш технологічно розвинені країни, наприклад Сполучені Штати Америки, мають значний власний досвід формування національної стратегії захисту кіберпростору, у тому числі на доктринальному, державному рівні. Так, Національна стратегія захисту кіберпростору США була прийнята ще у 2003 році, коли наша країна перебувала на етапі інституціоналізації та нормативно-правового оформлення (другий етап).

Для вдосконалення та підвищення рівня організаційно-правового забезпечення у досліджуваній галузі доцільним вбачається опрацювання позитивного зарубіжного досвіду з урахуванням вітчизняних реалій.

На даному етапі було прийнято нову Директиву NIS2 — оновлений закон Європейського Союзу (Директива (ЄС) 2022/2555), який посилює кібербезпеку в державах-членах, вимагаючи від критично важливих та значущих організацій впроваджувати заходи з управління ризиками, повідомляти про інциденти безпеки та забезпечувати безпеку ланцюгів постачання. Вона розширює сферу застосування оригінальної Директиви NIS, охоплюючи більше секторів, посилює повноваження органів влади щодо забезпечення дотримання законодавства та сприяє більш тісній співпраці через мережу груп реагування на інциденти комп'ютерної безпеки (CSIRT) та мережу EU-CyCLONe для управління великомасштабними кризами.

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 34(63). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 34(63). Category «B»
https://doi.org/10.58442/3041-1858-2025-34(63)

Також, про відповідність застосування в Україні міжнародних практик в поточних оцінках та протидії загрозам у кіберпросторі та загрозі зловмисних інформаційних проявів свідчить формат аналізу загроз у щорічній «Оцінці загроз розвідувального співтовариства США за 2025 рік» (ATA), опублікованому на веб-сайті Офіса Директора Національної розвідки США у березні 2025 року [6].

У зазначеному документі висвітлюються основні загрози, що стоять перед США, з акцентом на таких основних державних супротивниках, як Китай, Росія, Іран і Північна Корея, а також транснаціональних злочинних організаціях і терористичних угрупованнях. У звіті детально описано, як ці суб'єкти використовують такі методи, як кібердіяльність, військова модернізація та проксі-групи, щоб кинути виклик інтересам США.

Слід відмітити, що кожний із зазначених спротивів США, де є Росія – країна-агресор для України, а також фактичні союзники Росії у військовій агресії (Північна Корея та Іран) оцінюються за напрямами: військова справа (та її модернізація), кіберпростір, зловмисні заходи впливу, зброя масового ураження, використання космосу, технології та економічні фактори. Фактично, «кіберпростір» та «зловмисні заходи впливу» – це окремі напрями негативних загроз, що обумовлює різні напрями визначення, оцінювання та протидії настанню їх негативних наслідків.

Характеризуючи загрози у кіберпросторі зі сторони Росії, відзначається, що передові кіберможливості Росії, її неодноразові успіхи у збиранні розвідданих з важливих об'єктів та минулі спроби заздалегідь забезпечити собі доступ до критичної інфраструктури США (інтерпретуємо – й критичної інфраструктури України) роблять її постійною загрозою для контррозвідки та кібератак.

Унікальною сильною стороною Москви (Росії) є практичний досвід, набутий у процесі інтеграції кібератак та операцій з військовими діями в умовах війни, що, майже напевно, посилює її потенціал зосередити комбінований вплив на об'єкти США в умовах конфлікту. Протягом останнього десятиліття Росія продемонструвала реальні можливості з дестабілізації, зокрема набула досвіду в здійсненні атак, безперервно атакуючи мережі України дестабілізуючим та руйнівним шкідливим програмним забезпеченням [6, с. 19–20].

Характеризуючи зловмисні заходи впливу зі сторони Росії, серед іншого зазначено, що Москва (Росія) використовує заходи впливу для підриву підтримки Заходу Україні та поширюючи вигідні для Росії наративи. Зловмисні заходи впливу Москви (Росії) триватимуть у

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 34(63). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 34(63). Category «B»
https://doi.org/10.58442/3041-1858-2025-34(63)

найближчому майбутньому і, майже напевно, стануть більш витонченими та масштабними [6, с. 20].

За результатами вивчення можливо визначити основні тенденції щодо організаційно-правового забезпечення інформаційної безпеки в енергетичній сфері в Україні:

- трансформація первинних декларативних засад до конкретних інституційних механізмів регулювання;
- європейська інтеграція як визначальний вектор формування сучасної системи інформаційної безпеки в енергетичній сфері в Україні;
- постійний вплив зовнішніх загроз та кризових факторів на розвиток організаційно-правового забезпечення інформаційної безпеки в енергетичній сфері;
- актуальність механізмів публічного управління у кризових умовах через форми публічно-приватного партнерства у сфері енергетичної безпеки, мобілізацію державних і приватних ресурсів.

МЕТОДИ ДОСЛІДЖЕННЯ / RESEARCH METHODS

Для вирішення поставленої мети використано теоретичні методи наукового дослідження: історичний (хронологічний) та функціональний методи, аналіз чинних нормативно-правових актів; емпіричні методи: спостереження та порівняння; комплексні методи: абстрагування, аналіз і синтез, елементарно теоретичний, та інші методи досліджень.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ / RESEARCH RESULTS

У публікації наведено результатами дослідження щодо попереднього аналізу сучасного стану проблемних питань організаційно-правового забезпечення інформаційної безпеки в енергетичній сфері.

Окреслено періодизацію становлення та розвитку організаційно-правового забезпечення інформаційної безпеки в енергетичній сфері в Україні на основі значимих правових подій.

За зібраними даними проаналізовано тенденції розвитку організаційно-правового забезпечення інформаційної безпеки в енергетичній сфері в Україні як об’єкта публічного регуляторного впливу.

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 34(63). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 34(63). Category «B»
https://doi.org/10.58442/3041-1858-2025-34(63)

ВИСНОВКИ / CONCLUSIONS

У результаті теоретичного аналізу встановлено, що проблемні питання та негативні фактори, які впливають на розвиток організаційно-правового забезпечення інформаційної безпеки в енергетичній сфері, є стійкими, але їх негативний вплив можливо мінімізувати.

Військова агресія Російської Федерації стала додатковим каталізатором змін та управлінських дій у цій сфері, внаслідок реалізації нових нормативно-правових актів України, обумовлених цією агресією.

Майбутній розвиток організаційно-правового забезпечення інформаційної безпеки в енергетичній сфері в Україні пов'язаний із інтеграцією з міжнародними стандартами (міжнародні стандарти ISO/IEC у сфері інформаційної безпеки, європейська директива NIS2 Directive).

Перспективи подальших досліджень у цьому напрямі / Prospects for further research in this direction. Представлені результати досліджень є початковою ланкою в обґрунтування теоретико-методологічних засад організаційно-правових механізмів та інструментів забезпечення інформаційної безпеки в енергетичній сфері в Україні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ / REFERENCES

[1] В. М. Бутузов, В. Д. Гавловський, А. В. Корягін, «Несанкціонований доступ до комп’ютерних мереж як явище та правова категорія: умови існування та організація протидії», *Боротьба з організованою злочинністю та корупцією (теорія і практика)*, вип. 16, с. 239–250, 2007.

[2] T. Brewster «Ukraine Claims Hackers Caused Christmas Power Outage». (укр. – “Україна стверджує, що хакери спричинили перебої з електропостачанням на Різдво”), *Forbes Magazine.* [Електронний ресурс]. Доступно: https://www.forbes.com/sites/thomasbrewster/2016/01/04/ukraine-power-out-cyber-attack/ Дата звернення: Верес. 03, 2025.

[3] О. О. Резнікова, К. Є. Войтовський, А. В. Лепіхо, «Організація системи забезпечення національної стійкості на регіональному і місцевому рівнях», *Аналітична доповідь. Центр безпекових досліджень*, 2021. с. 84-85. [Електронний ресурс]. Доступно: https://niss.gov.ua/sites/default/files/2021-09/analytrep_08_2021.pdf Дата звернення: Верес. 03, 2025.

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 34(63). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 34(63). Category «B»
https://doi.org/10.58442/3041-1858-2025-34(63)

[4] Кабінет Міністрів України. (2025, Берез. 07). *Розпорядження № 204-р «Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України».* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text

[5] Верховна Рада України. (2022, Берез. 16). *Закон № 2149-IX «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану».* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/2149-20#Text

[6] Annual Threat Assessment of the U.S. Intelligence Community, Office of the Director of National Intelligence (укр. – Щорічна оцінка загроз розвідувального співтовариства США, Офіс Директора Національної розвідки США). [Електронний ресурс]. Доступно: https://www.intelligence.gov/annual-threat-assessment Дата звернення : Верес. 03, 2025.

Матеріал надійшов до редакції 20.10.2025 р.

PERIODIZATION OF FORMATION AND DEVELOPMENT OF ORGANIZATION AND LEGAL SUPPORT FOR ENSURING INFORMATION SECURIRY IN THE ENERGY SECTOR OF UKRAINE

Artem Koriahin,
Postgraduate student of the Department of
Public Administration and Project Management
Educational and Scientific Institute of Management and Psychology.
SIHE «University of Educational Management».
Kyiv, Ukraine.
a_koryagin@ukr.net

Abstract. The publication presents the results of a preliminary analysis of current challenges in the organizational and legal framework for ensuring information security in the energy sector. It outlines the periodization of the formation and development of organizational and legal support for information security in Ukraine's energy sector, based on significant legal events. Using the collected data, the study analyzes the trends in the evolution of organizational and legal mechanisms for information security in the energy sector as an object of public regulatory influence. Key legal milestones are identified, along with the specific features and effective

factors characterizing each period. The military aggression of the Russian Federation has acted as an additional catalyst for changes and managerial actions in this domain, leading to the adoption of new regulatory acts in Ukraine necessitated by the aggression. The future development of organizational and legal mechanisms for ensuring information security in the energy sector of Ukraine is closely connected with integration into international standards (in particular, ISO/IEC standards in the field of information security and the European NIS2 Directive). The findings presented constitute an initial step toward substantiating the theoretical and methodological foundations of organizational and legal mechanisms and instruments for safeguarding information security in Ukraine's energy sector.

Keywords: information security; public regulation; organizational and legal support; cyberspace and cybersecurity.

ПЕРЕКЛАД, ТРАНСЛІТЕРАЦІЯ / TRANSLATED AND TRANSLITERATED

[1] V. M. Butuzov, V. D. Havlovskyi, A. V. Koriahin, «Nesanktsionovanyi dostup do kompiuternykh merezh yak yavyshche ta pravova katehoriia: umovy isnuvannia ta orhanizatsiia protydii», Borotba z orhanizovanoiu zlochynnistiu ta koruptsiieiu (teoriia i praktyka), vyp. 16, s. 239–250, 2007. (in Ukrainian).

[2] T. Brewster «Ukraine Claims Hackers Caused Christmas Power Outage». Forbes Magazine. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2016/01/04/ukraine-power-out-cyber-attack/ Application date: September 03, 2025. (in English).

[3] O. O. Reznikova, K. Ye. Voitovskyi, A. V. Lepikho, «Orhanizatsiia systemy zabezpechennia natsionalnoi stiikosti na rehionalnomu i mistsevomu rivniakh», Analitychna dopovid. Tsentr bezpekovykh doslidzhen, 2021. s. 84–85. [Elektronnyi resurs]. Dostupno: https://niss.gov.ua/sites/default/files/2021-09/analytrep_08_2021.pdf Data zvernennia: Veres. 03, 2025. (in Ukrainian).

[4] Kabinet Ministriv Ukrainy. (2025, Berez. 07). Rozporiadzhennia № 204-r «Pro zatverdzhennia planu zakhodiv na 2025 rik z realizatsii Stratehii kiberbezpeky Ukrainy». [Elektronnyi resurs]. Dostupno: https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text (in Ukrainian).

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 34(63). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 34(63). Category «B»
https://doi.org/10.58442/3041-1858-2025-34(63)

[5] Verkhovna Rada Ukrainy. (2022, Berez. 16). Zakon № 2149-IX «Pro vnesennia zmin do Kryminalnoho kodeksu Ukrainy shchodo pidvyshchennia efektyvnosti borotby z kiberzlochynnistiu v umovakh dii voiennoho stanu». [Elektronnyi resurs]. Dostupno: https://zakon.rada.gov.ua/laws/show/2149-20#Text (in Ukrainian).

[6] Annual Threat Assessment of the U.S. Intelligence Community, Office of the Director of National Intelligence [Online]. Available: https://www.intelligence.gov/annual-threat-assessment Application date: September 03, 2025. (in English).

Retrieved October 20, 2025 отримано
Reviewed October 31, 2025 рецензовано
Published November 26, 2025 опубліковано