Міністерство внутрішніх справ України
ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ
ФАКУЛЬТЕТ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ ОРГАНІВ
ДОСУДОВОГО РОЗСЛІДУВАННЯ НАЦІОНАЛЬНОЇ
ПОЛІЦІЇ УКРАЇНИ
КАФЕДРА КРИМІНАЛЬНОГО ПРАВА ТА КРИМІНОЛОГІЇ
ГОЛОВНЕ СЛІДЧЕ УПРАВЛІННЯ
НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

КВАЛІФІКАЦІЯ ОКРЕМИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ПРОТИ КРИТИЧНО ВАЖЛИВИХ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ (ст. ст. 259, 360 КК України)

Методичні рекомендації

Колектив авторів

Дніпро
2024

УДК 343.32/34
К 32

Схвалено Науково-методичною радою
Дніпровського державного
університету внутрішніх справ
(протокол № 12 від 19.06.2024)

РЕЦЕНЗЕНТИ:

доктор юридичних наук, професор **Ігор Медицький,** професор кафедри політики у сфері боротьби зі злочинністю та кримінального права Прикарпатського національного університету імені Василя Стефаника;

Оксана Матвієнко, заступник начальника відділу розслідування злочинів, скоєних проти життя та здоров'я особи, Слідчого управління ГУНП в Дніпропетровській області, підполковник поліції.

К 32 **Кваліфікація окремих кримінальних правопорушень проти критично важливих об'єктів інфраструктури (ст. ст. 259, 360 КК України)** : метод. рекомендації / кол. авт. Дніпро : ДДУВС, 2024. 132 с.

ISBN 978-617-560-007-8

Методичні рекомендації підготовлено з ініціативи авторського колективу кафедри кримінального права та кримінології Дніпровського державного університету внутрішніх справ з метою надання науково-обґрунтованих рекомендацій щодо кваліфікації окремих кримінальних правопорушень проти критично важливих об'єктів інфраструктури.

У межах методичних рекомендацій, на досягнення їх мети авторами визначено поняття об'єктів критичної інфраструктури, розглянуто правове регулювання захисту та правового режиму об'єктів критичної інфраструктури в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, особливого періоду та кваліфікацію окремих кримінальних правопорушень проти критично важливих об'єктів інфраструктури (ст. 259, 360 КК України).

Можуть бути використані як навчальний матеріал в начальному процесі ЗВО України з особливими умовами навчання для здобуття знань, напрацювання навичок майбутніми поліцейськими (курсантами) та поліцейськими (в межах підвищення кваліфікації) щодо кваліфікації окремих кримінальних правопорушень проти критично важливих об'єктів інфраструктури.

ISBN 978-617-560-007-8

ЗМІСТ

АВТОРСЬКИЙ КОЛЕКТИВ

Василь БЕРЕЗНЯК – завідувач кафедри кримінального права та кримінології факультету підготовки фахівців для органів досудового розслідування Національної поліції України Дніпровського державного університету внутрішніх справ, доктор юридичних наук, старший науковий співробітник;

Владислав БУРЛАКА – начальник відділу Головного слідчого управління Національної поліції України, кандидат юридичних наук;

Валентин ЛЮДВІК – доцент кафедри кримінального права та кримінології факультету підготовки фахівців для органів досудового розслідування Національної поліції України Дніпровського державного університету внутрішніх справ, кандидат юридичних наук, доцент;

Ельвіра СИДОРОВА – заступник директора факультету підготовки фахівців для органів досудового розслідування Національної поліції України Дніпровського державного університету внутрішніх справ, доктор юридичних наук, доцент;

Олексій ТИТАРЕНКО – старший науковий співробітник лабораторії з підготовки військ Київського інституту Національної гвардії України, доктор юридичних наук, доцент;

Юлія ТКАЧ – ад'юнкт кафедри кримінального права та кримінології факультету підготовки фахівців для органів досудового розслідування Національної поліції України Дніпровського державного університету внутрішніх справ.

ПЕРЕДМОВА

В умовах збройної агресії російської федерації проти України ворогом постійно змінюється тактика ведення бойових дій, включно з ракетними обстрілами міст, об'єктів критичної інфраструктури. Постійно ворогом здійснюються кібератаки на сайти державних установ, банківські установи, об'єкти телекомунікацій та інші об'єкти критичної інфраструктури. Багато шкоди національній та державній безпеці завдає інформаційна війна, яка також ведеться спецслужбами країни-агресорки проти України, що має на меті посіяти паніку серед цивільного населення, підвищення рівня недовіри до чинної влади, військового керівництва країни.

Також окремою проблемою залишається діяльність на нашій території диверсійно-розвідувальних груп противника, розгалуженої мережі агентів ФСБ, наявність серед українського населення прихильників «руського миру» («ждунів»), які на замовлення ворожої сторони проводять диверсійну роботу, яка останнім часом спрямована на виявлення, пошкодження та знищення саме об'єктів критичної інфраструктури.

Щодо останнього, то відповідно до Закону України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX до таких об'єктів відносять об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам.

Будь-яке суспільно небезпечне посягання на об'єкти критичної інфраструктури має тягти за собою, як наслідок, кримінально-правову відповідальність осіб, винних у вчиненні таких дій. Наприклад, наявна офіційна статистика офісу ГПУ вказує на поступову тенденцію за останні три роки щодо збільшення кримінальних правопорушень, вчинених проти об'єктів критичної інфраструктури, відповідальність за які передбачена ст. ст. 259, 360 КК України.

Водночас попередній аналіз судово-слідчої практики застосування цих норм вказує на певну їх неоднозначність та стабільність, що зумовлено специфікою визначення об'єктивних ознак цих

складів кримінальних правопорушень, а також змінами стосовно цих норм останнім часом.

Разом з вирішенням питань правильної кваліфікації за суспільно-небезпечні посягання на об’єкти критичної інфраструктури є актуальним розгляд й інших питань, зокрема, які стосуються:

1) конкретизації змісту понять «об’єкти критичної інфраструктури», «об’єкти критичної інформаційної інфраструктури»;

2) дослідження змісту поняття «критичної інфраструктури» в країнах Європейського Союзу та його узгодженість з поняттям, закріпленого в чинному національному законодавстві;

3) визначення системи національних суб’єктів, які уповноважені забезпечувати безпеку на об’єктах критичної інфраструктури як в мирний час, так і в особливий період, під час запровадження надзвичайного та воєнного станів, введення надзвичайної ситуації;

4) визначення компетенції та спроможностей Національної поліції України, Національної гвардії України, Державної служби з надзвичайних ситуацій, Служби безпеки України у профілактиці та запобіганні кримінальним правопорушенням, які посягають на об’єкти критичної інфраструктури. Дослідження окремих питань потребуватиме виконання окремих наукових розвідок надалі.

Розділ 1
ПОНЯТТЯ «ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ»

Сьогодні від об'єктів критичної інфраструктури залежать майже всі сфери життєдіяльності людини, суспільства та держави, що робить цю тематику дослідження актуальною в глобальному масштабі. Однак треба зазначити, що в умовах воєнного стану та війни з рф руйнування об'єктів критичної інфраструктури є цілеспрямованим. Крім того, об'єкти критичної інфраструктури, що працюють у всіх сферах життєзабезпечення міст, регіонів та країни загалом, найчастіше стають об'єктами кібератак.

За статистичними даними, на основі звітів за період з 2013 по 2023 роки, оприлюднених на офіційних сайтах офісу Генерального прокурора України та Державної судової адміністрації щодо кримінальних правопорушень, вчинених проти об'єктів критичної інфраструктури, передбачених ст. 259, 360 КК України та поданих у вигляді візуалізації.

Об'єкти критичної інфраструктури – це стратегічно важливі підприємства та установи, без яких неможливе функціонування суспільства та економіки країни. Їх незапланована зупинка, перебої в роботі або повне руйнування можуть становити загрозу для державної безпеки та природного середовища, послабити обороноздатність, призвести до матеріальних і фінансових втрат або навіть спричинити людські жертви[1].

У Законі України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX визначено термін **об'єкти критичної інфраструктури** так: об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам[2].

Стосовно юридичного визначення, то законодавча база європейських країн у сфері захисту критичної інфраструктури містить різний перелік життєво важливих (критичних) інфраструктур (об'єктів). Він визначається відповідно до їхніх традицій, суспільних та політичних переконань, а також географічних та історичних особливостей кожної держави. Важливою частиною критичної інфраструктури є їх інформаційна складова – критична інформаційна інфраструктура.

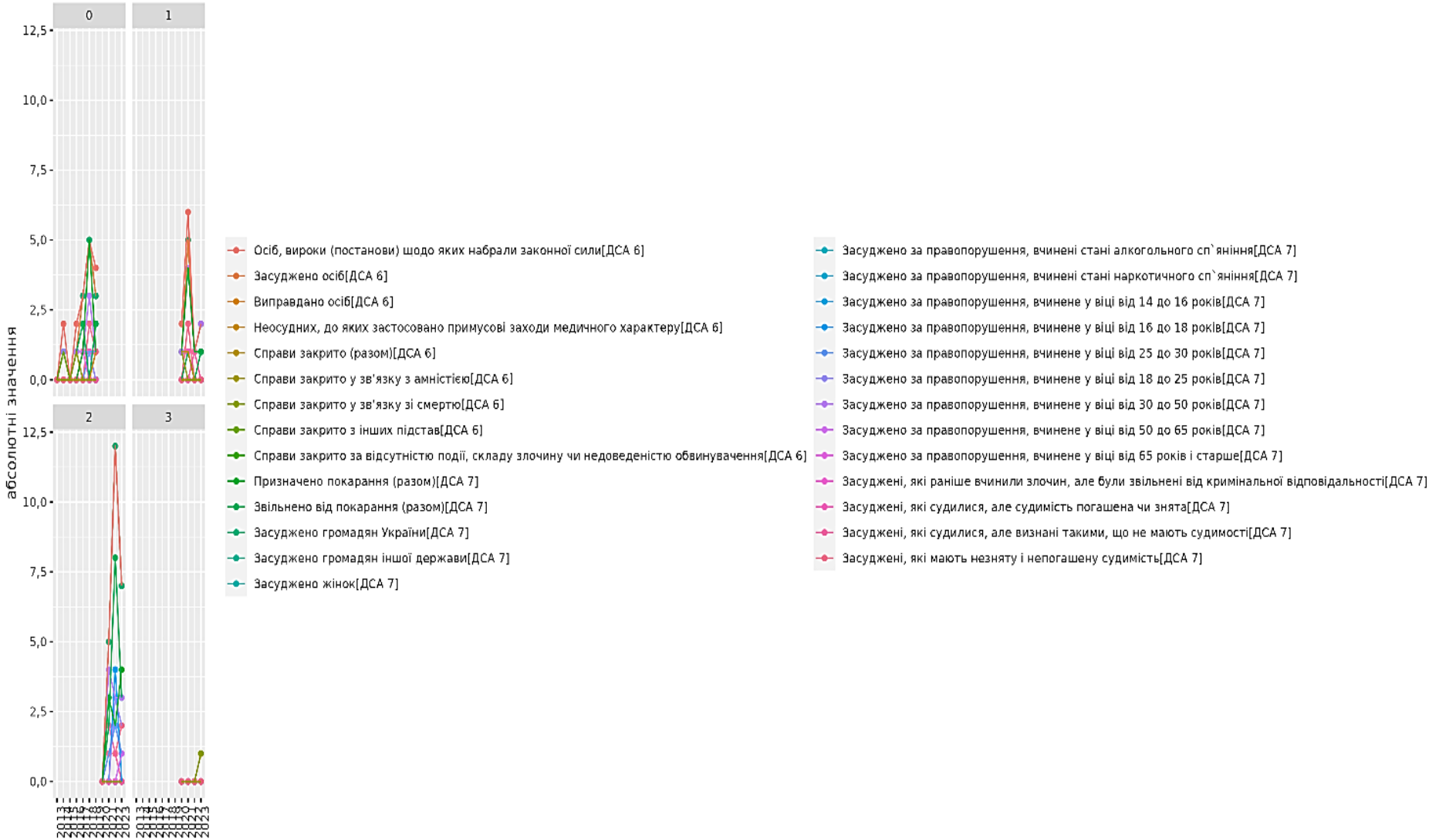
---

[1] Що таке об'єкти критичної інфраструктури. SmartTender. URL : https://smarttender.biz/terminy/view/ob-yekti-kritichnoyi-infrastrukturi/

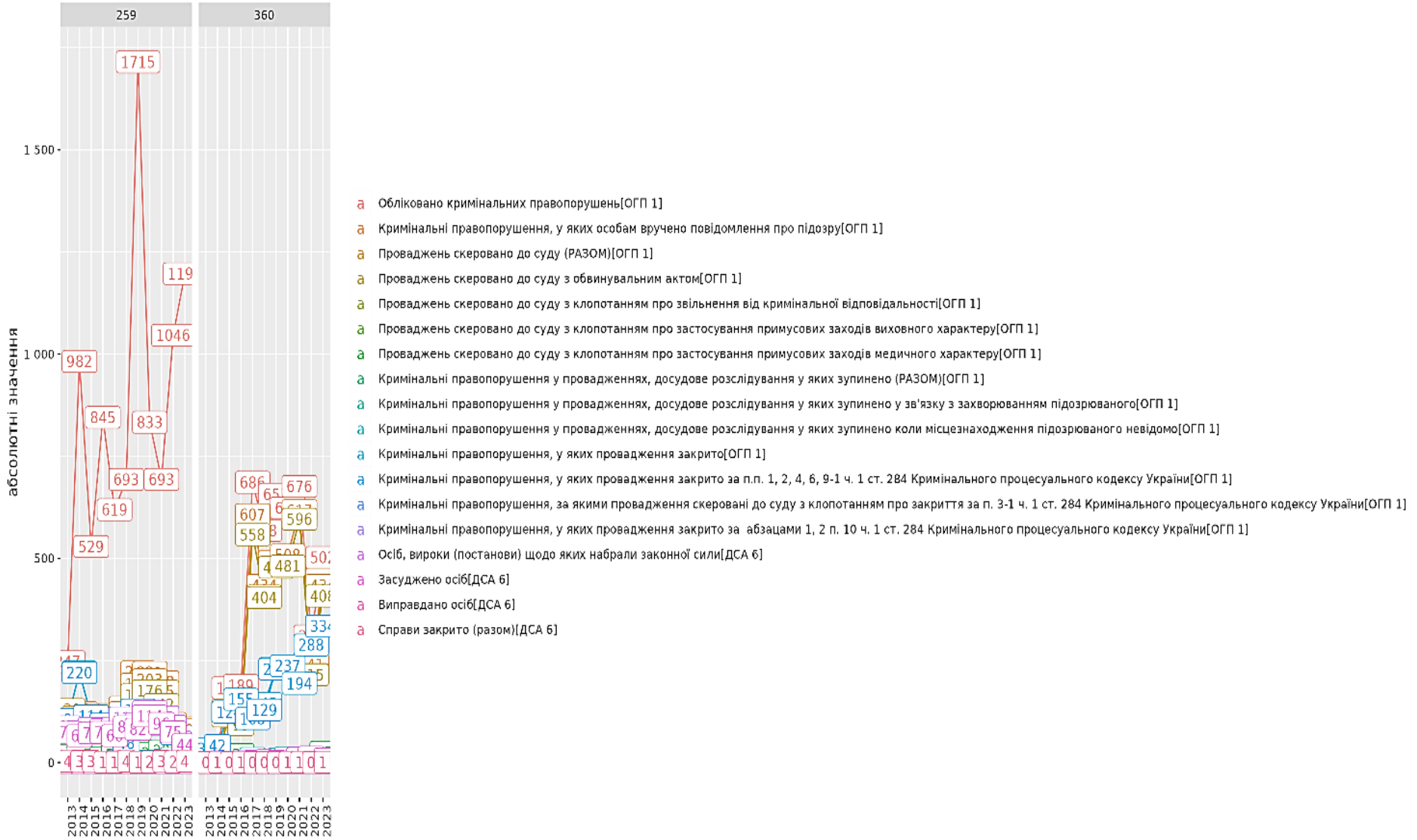
[2] Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL : https://zakon.rada.gov.ua/ laws/show/1882-20#Text.

Візуалізація на підставі звітів за період з 2013 по 2023 рік, представлених на
офіційних сайтах Офісу Генерального прокурора України та Державної судової адміністрації.
Створено у веб-застосунку - Карчевський М. В. Протидія злочинності в Україні: інфографіка : інтерактивний довідник.
URL :https://karchevskiy.org/i-dovidnyk/ (дата звернення : 26.05.2024)
Стаття 259. Завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності
(дані по частинах статті у відсотковому представленні)

Візуалізація на підставі звітів за період з 2013 по 2023 рік, представлених на
офіційних сайтах Офісу Генерального прокурора України та Державної судової адміністрації.
Створено у веб-застосунку - Карчевський М. В. Протидія злочинності в Україні: інфографіка : інтерактивний довідник.
URL :https://karchevskiy.org/i-dovidnyk/ (дата звернення : 26.05.2024)
Стаття 360. Умисне пошкодження або руйнування телекомунікаційної мережі (дані по частинах статті)



Візуалізація на підставі звітів за період з 2013 по 2023 рік, представлених на
офіційних сайтах Офісу Генерального прокурора України та Державної судової адміністрації.
Створено у веб-застосунку - Карчевський М. В. Протидія злочинності в Україні: інфографіка : інтерактивний довідник.
URL :https://karchevskiy.org/i-dovidnyk/ (дата звернення : 26.05.2024)



Наприклад, ось перелік країн, де в нормативно-правових документах використовується термін **«критична інфраструктура»** (critical infrastructure) для визначення життєво важливих інфраструктур (об'єктів)[3].

Країна	Визначення	Нормативно-правова база
Визначення відповідно до Директиви Ради 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію і позначення Європейських критичних інфраструктур та оцінку необхідності вдосконалення їх захисту	**Критична інфраструктура** – це актив, система чи її частина, розташовані в країні-члені ЄС, є необхідними об'єктами для підтримки життєво важливих суспільних функцій, охорони здоров'я, безпеки, економічного та соціального добробуту людей. **Європейська критична інфраструктура** – це об'єкт критичної інфраструктури, розташований в державах-членах, порушення функціонування або знищення якого матиме значний вплив, принаймні, на дві держави-члени.	COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection[4]
Австрія	Природні ресурси, послуги, інформаційні технології, мережі, а також інші активи, які в разі порушення або руйнування можуть серйозно вплинути на здоров'я, безпеку, економічний добробут громадян або на ефективне функціонування уряду.	Austrian Program on Critical Infrastructure Protection (APCIP)[5]
Великобританія	Активи, послуги та системи, що підтримують економічне, політичне й соціальне життя Великобританії, втрата яких	Strategic Framework and Policy Statement on Improving the Resilience of Critical

[3] Об'єкти критичної інфраструктури та об'єкти критичної інформаційної інфраструктури в європейських країнах. Інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром на запит Апарату Верховної Ради України. URL : https://infocenter.rada.gov.ua/uploads/documents/29297.pdf.

[4] COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. URL : http://eur-lex.europa.eu/ LexUriServ/LexUriServ.do?uri= OJ:L:2008:345:0075:0082:EN:PDF.

[5] Legislative Framework for CIP in Austria. URL : https://cipworkshopevents/wp-content/uploads/2017/10/S4-T2-Legislative_Framework_for_CIP_in_Austria.pdf.

Країна	Визначення	Нормативно-правова база
	може: 1) спричинити масштабну загибель людей; 2) відчутно вплинути на національну економіку; 3) призвести до інших серйозних соціальних наслідків; 4) перетворитись на одне з невідкладних завдань національного уряду.	Infrastructure to Disruption from Natural Hazards[6]
Нідерланди	Продукти, послуги та супровідні процеси (програмне забезпечення, апаратні засоби й дані), які в разі порушення або відмови, можуть викликати серйозні соціальні негаразди – величезні жертви або серйозні економічні збитки.	The policy letter Protecting Critical Infrastructure[7]
Німеччина	Конструкції, системи, необхідні для підтримання найважливіших функцій суспільства, постійна доступність яких гарантує кожному члену суспільства почуття власної та громадської безпеки.	The National Strategy for Critical Infrastructure Protection (CIP Strategy)[8]
Швейцарія	Інфраструктура, порушення, відмова або руйнування якої може істотно вплинути на здоров'я населення, громадські справи, навколишнє середовище, безпеку та соціально-економічний добробут.	National strategy for the protection of Switzerland against cyber risks[9]

[6] Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards. URL : https://www.gov.uk/ government/uploads/system/uploads/attachment_data/file/62504/ strategic-framework.pdf.

[7] The policy letter Protecting Critical Infrastructure. URL : https://english.nctv.nl/binaries/20150409-national-security-progress-letter-national-safety-2015_tcm32-84272.pdf.

[8] National Strategy for Critical Infrastructure Protection (CIP Strategy). URL : http://ccpic.mai.gov.ro/docs/ Germania_cip_stategy.pdf.

[9] National strategy for the protection of Switzerland against cyber risks. URL : https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncssmap/National_ strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf.

Країна	Визначення	Нормативно-правова база
Бельгія	Інсталяція, система або її частина, що має значення державного масштабу, є важливим для підтримки життєво важливих суспільних функцій, охорони здоров'я, безпеки, безпеки економічного та соціального добробуту людей, і якщо вони будуть порушені або знищені, це матиме значний вплив на країну.	Law of 1 July 2011 on the security and protection of critical infrastructures [10]
Чехія	Системи та послуги, нефункціональність яких призведе до серйозного впливу на державну безпеку, її економіку, державне управління та забезпечення основних повсякденних потреб населення.	Regulation № 317/2014 Coll. on the Determination of Important Information Systems and their Determination Criteria[11]
Португалія	Компонент, система чи її частина, розташована на національному рівні, яка необхідна для підтримки життєдіяльності суспільства, здоров'я, безпеки та добробуту економічного або соціального характеру, а також порушення або знищення, матимуть суттєвий вплив на країну, якщо врахувати неможливість продовжувати виконувати ці функції.	The Act for National Security and the Safeguarding and Defence of Classified Material (SEGNAC 1)[12]

[10] Law of 1 July 2011 on the security and protection of critical infrastructures. URL : https://www.nbb.be/en/ articles/law-1-july-2011-security-and-protection-criticalinfrastructures-inofficial-translation.

[11] Regulation No. 317/2014 Coll. on the Determination of Important Information Systems and their Determination Criteria. URL : https://nukib.gov.cz/download/ publications_en/legislation/Decree_317_2014_EN_v1.0_final.pdf.

[12] The Act for National Security and the Safeguarding and Defence of Classified Material (SEGNAC 1). URL : www.gns.gov.pt/media/1356/SEGNAC1.pdf.

Країна	Визначення	Нормативно-правова база
Іспанія	Стратегічні інфраструктури (тобто ті, які забезпечують основні послуги), функціонування яких є необхідним та немає альтернативи, порушення або руйнування матимуть серйозний вплив на основні послуги в країні.	Law 8/2011 on the Measures for the Protection of Critical Infrastructure 2011[13]

Отже, критична інформаційна інфраструктура розглядається як центральний компонент у критичній інфраструктурі різних держав, що відображено у відповідних визначеннях цього терміну. Основні причини критичності інформаційної складової інфраструктури випливають зі стрімкого поширення інформаційних технологій в всіх сферах людської діяльності, що призводить до залежності від них громадян, суспільства та держави, а також до підвищення вразливості та потенційних загроз різного характеру. Відсутність поняття ***«критична інформаційна інфраструктура»*** в законодавстві багатьох держав пояснюється тим, що інформаційна складова входить до обсягу поняття інфраструктури в цілому (тобто критичної інфраструктури) і не виділяється як певна ланка. Наприклад, Нідерланди та Великобританія виробили спільне розуміння критичної інформаційної інфраструктури як «***інформаційні системи***» (програмне забезпечення, апаратні засоби й дані) та послуги, які підтримують один або декілька найважливіших об'єктів інфраструктури, порушення роботи або відімкнення яких завдає серйозної шкоди функціонуванню залежної критичної інфраструктури[14].

До об'єктів критичної інфраструктури належить: урядування та надання найважливіших публічних (адміністративних) послуг; енергозабезпечення (зокрема постачання теплової енергії); водопостачання та водовідведення; продовольче забезпечення; охорона здоров'я; фармацевтична промисловість; виготовлення вакцин, стале функціонування біолабораторій; інформаційні послуги; електронні комунікації; фінансові послуги; транспортне забезпечення; оборона, державна безпека; правопорядок, здійснення правосуддя, тримання під вартою; цивільний захист населення та територій, служби порятунку;

[13] Law 8/2011 on the Measures for the Protection of Critical Infrastructure 2011. URL : http://www.boe.es/boe/ dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf.

[14] International critical information infrastructure protection handbook. URL : https://subs.emis.de/LNI/Proceedings/ Proceedings36/GI-Proceedings.36-7.pdf

космічна діяльність, космічні технології та послуги; хімічна промисловість; дослідницька діяльність[15].

Постановою КМУ № 1109 від 09.10.2020 «Деякі питання об'єктів критичної інфраструктури» затверджено порядок віднесення об'єктів до критичної інфраструктури, а також перелік секторів критичної інфраструктури та методику категоризації об'єктів критичної інфраструктури[16].

Згідно з вказаною Постанови визначено перелік секторів критичної інфраструктури, до якого зокрема входять: паливно-енергетичний сектор; цифрові технології; захист інформації; харчова промисловість та агропромисловий комплекс; державний матеріальний резерв; охорона здоров'я; ринки капіталу та організовані товарні ринки; фінансовий сектор; транспорт і пошта; системи життєзабезпечення; промисловість; сектор громадської безпеки; цивільний захист населення і територій; охорона навколишнього природного середовища; сектор оборони; правосуддя; виконання кримінальних покарань, тримання під вартою та утримання військовополонених; державна реєстрація; наукові дослідження та розробки; фінансовий сектор; вибори та референдуми; соціальний захист; інформаційний сектор; державна влада та місцеве самоврядування. Усі вони відповідальні за певні сектори, підсектори та тип основних послуг об'єктів критичної інфраструктури держави, які зазначені в переліку.

Відповідно до ч. 2 ст. 10 Закону України «Про критичну інфраструктуру» встановлюються такі категорії критичності об'єктів критичної інфраструктури:

I категорія критичності – особливо важливі об'єкти, які мають загальнодержавне значення, суттєво впливають на інші об'єкти критичної інфраструктури та порушення функціонування яких призведе до виникнення кризової ситуації державного значення;

II категорія критичності – життєво важливі об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації регіонального значення;

III категорія критичності – важливі об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації місцевого значення;

IV категорія критичності – необхідні об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації локального значення[17].

---

[15] Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL : https://zakon.rada.gov.ua/ laws/show/1882-20#Text.

[16] Деякі питання об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 № 1109. URL : https://zakon.rada.gov.ua/laws/show/1109-2020-п#n42.

[17] Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL : https://zakon.rada.gov.ua/ laws/show/1882-20#Text.

У Законі України «Про критичну інфраструктуру» виділено основні суб'єкти у сфері критичної інфраструктури:

1) оператор критичної інфраструктури – юридична особа будь-якої форми власності та/або фізична особа – підприємець, що на правах власності, оренди або на інших законних підставах здійснює управління об'єктом критичної інфраструктури та відповідає за його поточне функціонування;

2) секторальний орган у сфері захисту критичної інфраструктури – державний орган, визначений законодавством відповідальним за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури;

3) уповноважений орган у сфері захисту критичної інфраструктури України забезпечує формування та реалізує державну політику у сфері захисту критичної інфраструктури, здійснює функціональне управління національною системою захисту критичної інфраструктури, забезпечує координацію діяльності міністерств та операторів критичної інфраструктури з питань забезпечення стійкості та захисту об'єктів критичної інфраструктури[18].

Однак для того щоб визначити, чи належить об'єкт до критичної інфраструктури, необхідно спочатку з'ясувати, хто уповноважений відносити об'єкти до об'єктів критичної інфраструктури.

Згідно з ч. 1 ст. 8 Закону України «Про критичну інфраструктуру», віднесення об'єктів до критичної інфраструктури здійснюється в порядку, встановленому Кабінетом Міністрів України.

Оскільки Кабінет Міністрів України не затвердив іншого, окремого Порядку віднесення об'єктів до критичної інфраструктури з моменту ухвалення Закону «Про критичну інфраструктуру», ми керуємося Порядком віднесення об'єктів до об'єктів критичної інфраструктури, що затверджений Постановою КМУ від 09.10.2020 № 1109 «Деякі питання об'єктів критичної інфраструктури».

Варто наголосити на тому, що у п. 4 вказаної Постанови секторальні органи у сфері захисту критичної інфраструктури, використовуючи перелік секторів критичної інфраструктури, ідентифікують об'єкти критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури. З огляду на це, секторальні органи у сфері захисту критичної інфраструктури разом з оператором критичної інфраструктури здійснюють категоризацію об'єктів критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури відповідно до Методики категоризації об'єктів критичної інфраструктури, затвердженої Постановою Кабінету

[18] Там само.

Міністрів України від 9 жовтня 2020 р. № 1109[19].

Тож відповідно до ст. 11 Закону України «Про критичну інфраструктуру» для цілей узгодження дій суб'єктів національної системи захисту критичної інфраструктури формується Реєстр об'єктів критичної інфраструктури. Збирання, узагальнення та попередній аналіз даних щодо об'єктів критичної інфраструктури та пропозиції щодо включення таких об'єктів до Реєстру в межах визначених секторів здійснюються секторальними органами у сфері захисту критичної інфраструктури. До речі, реєстр формується та ведеться уповноваженим органом у сфері захисту критичної інфраструктури України на основі пропозицій суб'єктів національної системи захисту критичної інфраструктури. Після включення об'єкта до Реєстру секторальні органи у сфері захисту критичної інфраструктури повідомляють про це оператора об'єкта критичної інфраструктури для забезпечення паспортизації та захисту об'єкта критичної інфраструктури відповідно до вимог Закону «Про критичну інфраструктуру». Сам порядок ведення Реєстру, включення об'єктів до Реєстру, доступ та надання інформації з нього визначається Кабінетом Міністрів України[20].

Згідно з ч. 6 ст. 11 Закону України «Про критичну інфраструктуру», інформація про об'єкти критичної інфраструктури, що міститься в Реєстрі, є відкритою, загальнодоступною та безоплатною, крім інформації з обмеженим доступом. Розпорядник забезпечує цілодобовий доступ до відкритої інформації Реєстру на своєму офіційному вебсайті[21].

Водночас, відповідно до п. 8 Постанови КМУ від 09.10.2020 № 1109 «Деякі питання об'єктів критичної інфраструктури», відомості про об'єкти критичної інфраструктури, що містяться у секторальних переліках об'єктів критичної інфраструктури, є інформацією з обмеженим доступом, захист якої забезпечується відповідно до вимог законодавства[22].

На тлі воєнного стану та війни з рф це виглядає абсолютно логічним і відповідає нормам, викладеним у ч. 2 ст. 6 (публічна інформація з обмеженим доступом) Закону України «Про доступ до публічної інформації» від 13.01.2011 № 2939-VI[23], оскільки оприлюднення інформації про перелік та адреси таких об'єктів критичної інфраструктури може мати негативні наслідки.

---

[19] Деякі питання об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 № 1109. URL : https://zakon.rada.gov.ua/laws/show/1109-2020-п#n42.

[20] Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL : https://zakon.rada.gov.ua/ laws/show/1882-20#Text.

[21] Там само.

[22] Деякі питання об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 № 1109. URL : https://zakon.rada.gov.ua/laws/show/1109-2020-п#n42.

[23] Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 27.05.2024).

Розділ 2
ЗАКОНОДАВСТВО ПРО КРИТИЧНУ ІНФРАСТРУКТУРУ ТА ЇЇ ЗАХИСТ. ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ТА ПРАВОГО РЕЖИМУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ, НАДЗВИЧАЙНОГО ТА ВОЄННОГО СТАНУ, ОСОБЛИВОГО ПЕРІОДУ

Критична інфраструктура завжди була важливою частиною національної безпеки в Україні, і законодавці швидко реагували на виклики у цій сфері. Об'єктом дослідження є відносини, що виникають у процесі функціонування національного правового механізму забезпечення безпеки об'єктів критичної інфраструктури.

Тож Закон України «Про критичну інфраструктуру» регулює відносини у сфері функціонування та захисту критичної інфраструктури в цілому та її об'єктів у мирний час. А саме: закони України «Про правовий режим воєнного стану», «Про правовий режим надзвичайного стану», «Про функціонування єдиної транспортної системи України в особливий період» та «Про оборону України», особливості захисту та правового режиму об'єктів критичної інфраструктури в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, а також в особливий період. Окремим законом регулюються відносини у сфері кіберзахисту та кібербезпеки об'єктів критичної інфраструктури[24]. Отже, законодавство у сфері кіберзахисту об'єктів критичної інформаційної інфраструктури регулюється такими нормативно-правовими актами:

– Постанова Кабінету Міністрів України від 19.06.2019 № 519 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»[25];

– Постанова Кабінету Міністрів України від 11.11.2020 № 1176 «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом»[26];

– Постанова Кабінету Міністрів України від 23.12.2020 № 1295

[24] Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL : https://zakon.rada.gov.ua/ laws/show/1882-20#Text.

[25] Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.2019 № 518. URL : https://zakon.rada.gov.ua/laws/show/518-2019-п#Text.

[26] Там само.

«Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки»[27];

– Постанова Кабінету Міністрів України від 29.12.2021 № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту»[28];

– Постанова Кабінету Міністрів України від 04.04.2023 № 299 «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі»[29];

– Постанова Кабінету Міністрів України від 16.05.2023 № 497 «Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж»[30];

– наказ адміністрації Держспецзв'язку від 02.12.2014 № 660 «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах»[31];

– наказ адміністрації Держспецзв'язку від 15.01.2016 № 20 «Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті»[32];

– Постанова Кабінету Міністрів України від 09.10.2020 № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури»[33];

– Постанова Кабінету Міністрів України від 09.10.2020 № 1109

---

[27] Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: Постанова Кабінету Міністрів України від 23.12.2020 № 1295. URL : https://zakon.rada.gov. ua/laws/show/1295-2020-п#Text.

[28] Про затвердження Положення про організаційно-технічну модель кіберзахисту: Постанова Кабінету Міністрів України від 29.12.2021 № 1426. URL : https://zakon.rada.gov.ua/laws/show/1426-2021-п#Text.

[29] Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Постанова Кабінету Міністрів України від 04.04.2023 № 299. URL : https://zakon.rada.gov.ua/laws/show/ 299-2023-п#Text.

[30] Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних: Постанова Кабінету Міністрів України від 16.05.2023 № 497. URL : https://zakon.rada.gov.ua/laws/show/497-2023-п#Text.

[31] Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних: наказ від 02.12.2014 № 660. URL : https:// zakon.rada.gov.ua/laws/show/z0090-15#n14.

[32] Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті: наказ від 15.01.2016 № 20. URL : https://zakon.rada.gov.ua/laws/show/z0196-16#n13.

[33] Деякі питання об'єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 № 943. URL : https://zakon.rada.gov.ua/laws/show/943-2020-п#n82.

«Деякі питання об’єктів критичної інфраструктури»[34];

– методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджені наказом Адміністрації Держспецзв’язку від 06.10.2021 № 601 (із змінами, внесеними згідно з наказами адміністрації Держспецзв’язку від 10.07.2022 № 343)[35];

– науково-практичний коментар до Положення про організаційно-технічну модель кіберзахисту, затвердженого постановою Кабінету Міністрів України від 29 грудня 2021 р. № 1426[36];

– наказ адміністрації Держспецзв’язку від 24.06.2022 № 284 «Про затвердження Порядку передачі комплектів обладнання підсистеми збору телеметрії інформаційно-комунікаційних систем (активні сенсори) системи виявлення вразливостей і реагування на кіберінциденти та кібератаки до об’єктів кіберзахисту»[37];

– наказ адміністрації Держспецзв’язку від 29.05.2023 № 463 «Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами»[38];

– наказ адміністрації Держспецзв’язку від 03.07.2023 № 570 «Про затвердження Методичних рекомендацій щодо реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі»[39];

---

[34] Деякі питання об’єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 № 1109. URL : https://zakon.rada.gov.ua/laws/show/1109-2020-п#Text.

[35] Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури: наказ адміністрації Держспецзв’язку від 06.10.2021 № 601 (зі змін.). URL : https://cip.gov. ua/ua/news/nakaz-ad-2021-10-06-601.

[36] Про затвердження Положення про організаційно-технічну модель кіберзахисту: Постанова Кабінету Міністрів України від 29.12.2021 № 1426. URL : https://zakon.rada.gov.ua/laws/show/1426-2021-п#Text.

[37] Про затвердження Порядку передачі комплектів обладнання підсистеми збору телеметрії інформаційно-комунікаційних систем (активні сенсори) системи виявлення вразливостей і реагування на кіберінциденти та кібератаки до об’єктів кіберзахисту: наказ адміністрації Держспецзв’язку від 24.06.2022 № 284. URL : https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-24-chervnya-2022-roku-284-pro-zatverdzhennya- poryadku-peredachi-komplektiv-obladnannya-pidsistemi-zbo.

[38] Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами: наказ адміністрації Держспецзв’язку від 29.05.2023 № 463. URL : https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-29-05-2023-463-pro-zatverdzhennya-metodichnikh- rekomendacii-shodo-zabezpechennya-kiberzakhistu-avtomatizovanikh-sistem-upravlinnya-tekhnologichnimi-procesami.

[39] Про затвердження Методичних рекомендацій щодо реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: наказ адміністрації Держспецзв’язку від 03.07.2023 № 570. URL : https://cip.gov.ua/ua/news/nakaz-administraciyi-

– наказ адміністрації Держспецзв'язку від 14.07.2023 № 599 «Про затвердження Примірної публічної пропозиції про здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж і Методичних рекомендацій з розроблення публічної пропозиції про здійснення пошуку та виявления потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж»[40];

– наказ адміністрації Держспецзв'язку від 30.08.2023 № 771 «Про затвердження Положення про систему захищеного доступу державних органів до мережі Інтернет»[41];

– наказ адміністрації Держспецзв'язку від 30.08.2023 № 773 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту систем електронного документообігу»[42];

– наказ адміністрації Держспецзв'язку від 02.09.2023 № 793 «Про затвердження форм подання відомостей до державного реєстру об'єктів критичної інформаційної інфраструктури»[43];

---

derzhspeczv-yazku-vid-03-07-2023-570-pro-zatverdzhennya-metodichnikh- rekomendacii-shodo-reaguvannya-sub-yektami-zabezpechennya-kiberbezpeki-na-rizni-vidi-podii-u-kiberprostori.

[40] Про затвердження Примірної публічної пропозиції про здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж і Методичних рекомендацій з розроблення публічної пропозиції про здійснення пошуку та виявления потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж: наказ адміністрації Держспецзв'язку від 14.07.2023 № 599. URL : https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-14-07-2023-599-pro-zatverdzhennya-primirnoyi-publichnoyi-propoziciyi-pro-zdiisnennya-poshuku-ta-viyavlennya-potenciinoyi-vrazlivosti.

[41] Про затвердження Положення про систему захищеного доступу державних органів до мережі Інтернет: наказ адміністрації Держспецзв'язку від 30.08.2023 № 771. URL : https://cip.gov.ua/ua/news/nakaz-administraciyi- derzhspeczv-yazku-pro-zatverdzhennya-polozhennya-pro-sistemu-zakhishenogo-dostupu-derzhavnikh- organiv-do-merezhi-internet-vid-30-serpnya-2023-roku-771.

[42] Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту систем електронного документообігу: наказ адміністрації Держспецзв'язку від 30.08.2023 № 773. URL : https://cip.gov.ua/ua/ news/nakaz-administraciyi-derzhspeczv-yazku-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-pidvishennya- rivnya-kiberzakhistu-sistem-elektronnogo-dokumentoobigu-vid-30-serpn.

[43] Про затвердження форм подання відомостей до державного реєстру об'єктів критичної інформаційної інфраструктури: наказ адміністрації Держспецзв'язку від 02.09.2023 № 793. URL : https://cip.gov.ua/ua/ news/nakaz-administraciyi-derzhspeczv-yazku-pro-zatverdzhennya-form-podannya-vidomostei-do-derzhavnogo-reyestru- ob-yektiv-kritichnoyi-informaciinoyi-infrastrukturi-vid-02-veres.

– наказ адміністрації Держспецзв'язку від 04.10.2023 № 877 «Про затвердження форми Плану захисту об'єкта критичної інфраструктури за проєктною загрозою національного рівня «кібератака/кіберінцидент»[44];

– наказ адміністрації Держспецзв'язку від 01 грудня 2023 року № 1011 «Про затвердження Рекомендацій з розроблення плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «кібератака/кіберінцидент»[45];

– форми надання відомостей до державного реєстру об'єктів критичної інформаційної інфраструктури[46];

– роз'яснення щодо заповнення форм надання відомостей до державного реєстру об'єктів критичної інформаційної інфраструктури[47];

– перелік документів міжнародних організацій та країн-партнерів у сфері кіберзахисту[48].

Крім того, захист критичної інфраструктури є невід'ємною частиною забезпечення національної безпеки України. Відповідно до п 2 ст. 4 Закону України «Про критичну інфраструктуру» державна політика у сфері захисту критичної інфраструктури ґрунтується на таких засадах:

1) визнання необхідності забезпечення безпеки та стійкості критичної інфраструктури;

2) визначення законодавчих вимог до принципів, пріоритетів, стратегічних завдань, підходів щодо захисту критичної інфраструктури;

---

[44] Про затвердження форми Плану захисту об'єкта критичної інфраструктури за проєктною загрозою національного рівня «кібератака/кіберінцидент: наказ адміністрації Держспецзв'язку від 04.10.2023 № 877. URL : https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-pro-zatverdzhennya-formi-planu- zakhistu-ob-yekta-kritichnoyi-infrastrukturi-za-proyektnoyu-zagrozoyu-nacionalnogo-rivnya-kiberataka.

[45] Про затвердження Рекомендацій з розроблення плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «кібератака/кіберінцидент: наказ адміністрації Держспецзв'язку від 01.12.2023 № 1011. URL : https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-01-grudnya-2023-roku-1011-pro-zatverdzhennya-richnogo-planu-zdiisnennya-zakhodiv-derzhavnogo-naglyadu-kontrolyu-u-sferi-doderzha.

[46] Про затвердження форм подання відомостей до державного реєстру об'єктів критичної інформаційної інфраструктури: наказ від 02.09.2023 № 793. URL : https://zakon.rada.gov.ua/rada/show/v0793519-23#Text.

[47] Роз'яснення щодо заповнення форм надання відомостей до державного реєстру об'єктів критичної інформаційної інфраструктури. URL : https://cip.gov.ua› api›attachment›download.

[48] Документи міжнародних організацій та країн-партнерів у сфері кіберзахисту. *Державна служба спеціального зв'язку та захисту інформації України*. URL : https://cip.gov.ua/ua/news/perelik-dokumentiv-mizhnarodnikh-organizacii-ta-krayin-partneriv-u-sferi-kiberzakhistu.

3) визначення суб'єктів національної системи захисту критичної інфраструктури, їх повноважень та засад відповідальності, порядку взаємодії;

4) створення умов та впровадження заходів, спрямованих на ефективне зниження і контроль за ризиками безпеки, на зниження ризику реалізації можливих загроз, ліквідацію та/або мінімізацію наслідків реалізованих загроз, кризових ситуацій та інших їх видів;

5) створення системи раннього виявлення загроз критичній інфраструктурі;

6) запровадження державно-приватного партнерства, взаємодії суб'єктів господарювання та населення з питань забезпечення захисту та стійкості критичної інфраструктури;

7) забезпечення міжнародного співробітництва у сфері захисту критичної інфраструктури;

8) створення умов швидкого відновлення надання життєво важливих функцій та послуг у разі реалізації загроз і порушення функціонування критичної інфраструктури[49].

До речі, суб'єктами національної системи захисту критичної інфраструктури є: Кабінет Міністрів України; апарат Ради національної безпеки і оборони України; Центральна виборча комісія; Національний банк України; Національна комісія з цінних паперів та фондового ринку, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг; адміністрація Державної служби спеціального зв'язку та захисту інформації України; Фонд державного майна України, інші центральні органи виконавчої влади зі спеціальним статусом; уповноважений орган у сфері захисту критичної інфраструктури України; центральний орган виконавчої влади, який забезпечує формування та реалізує державну політику у сфері цивільного захисту; секторальні та функціональні органи, інші міністерства та центральні органи виконавчої влади; Служба безпеки України; правоохоронні та розвідувальні органи, суб'єкти оперативно-розшукової та контррозвідувальної діяльності; Збройні Сили України, інші військові формування, утворені відповідно до законів України; місцеві органи виконавчої влади (військово-цивільні адміністрації – у разі утворення); органи місцевого самоврядування; оператори критичної інфраструктури; підприємства, установи та організації незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням

[49] Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL : https://zakon.rada.gov.ua/ laws/show/1882-20#Text.

безпеки та стійкості критичної інфраструктури[50].

Отже, забезпечення захисту та стійкості критичної інфраструктури здійснюється в таких режимах її функціонування:

- штатний режим;
- режим готовності та запобігання реалізації загроз;
- режим реагування на виникнення кризової ситуації;
- режим відновлення штатного функціонування[51].

Проте суб'єкти національної системи захисту критичної інфраструктури розробляють план взаємодії з іншими суб'єктами національної системи захисту, який погоджується з уповноваженим органом з питань захисту критичної інфраструктури України, затверджується Кабінетом Міністрів України та переглядається раз на три роки. У плані взаємодії можуть визначатися особливості взаємодії за режимами функціонування національної системи захисту критичної інфраструктури. Рішення про оголошення режимів функціонування критичної інфраструктури ухвалюють секторальні органи, у сфері захисту критичної інфраструктури – відповідальні за сектор критичної інфраструктури.

Однак уповноважений орган з питань захисту критичної інфраструктури України забезпечує формування та реалізацію державної політики у сфері захисту критичної інфраструктури, здійснює функціональне управління національною системою захисту критичної інфраструктури та координує діяльність міністерств та операторів критичної інфраструктури щодо забезпечення стійкості та захисту об'єктів критичної інфраструктури. Кабінет Міністрів України спрямовує, координує та контролює діяльність уповноваженого органу у сфері захисту критичної інфраструктури.

Захист критичної інфраструктури здійснюють такі органи:

– органи державної влади, визначені відповідальними за функціонування окремих державних систем захисту та реагування;

– державні органи, визначені відповідальними за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури;

– місцеві органи виконавчої влади (військово-цивільні адміністрації – у разі утворення) у сфері захисту критичної інфраструктури.

Щодо особливості діяльності окремих органів, відповідальних за формування та/або реалізацію державної політики у сфері захисту критичної інфраструктури, діяльність Національного банку України, уповноваженого органу у сфері захисту критичної інфраструктури

[50] Там само.
[51] Там само.

України, центрального органу виконавчої влади, що забезпечує формування та реалізує державну політику у сфері цивільного захисту, Служби безпеки України, Національної гвардії України, Національної поліції України, Збройних Сил України, Державної спеціальної служби транспорту та Державної служби спеціального зв'язку та захисту інформації України з питань формування та/або реалізації державної політики у сфері захисту критичної інфраструктури здійснюється в межах, визначених вищезгаданим Законом, та у порядку, встановленому законами України, що регламентують правові засади організації та діяльності зазначених у цій статті органів[52].

Основними завданнями операторів критичної інфраструктури є:

1) забезпечення захисту об'єктів критичної інфраструктури, зокрема створення, налагодження та підтримання функціонування ефективної системи фізичної безпеки, безпеки операційних систем та кібербезпеки;

2) розроблення, оновлення та забезпечення виконання об'єктових планів заходів щодо забезпечення безпеки і стійкості критичної інфраструктури, правил управління ризиками безпеки, планів локалізації та ліквідації наслідків аварій, а також заходів кіберзахисту;

3) проведення оцінки ризиків на об'єктах критичної інфраструктури та обмін інформацією про ризики та загрози з іншими суб'єктами національної системи захисту критичної інфраструктури, а також створення умов для належного виконання правоохоронними, розвідувальними та контррозвідувальними органами своїх завдань щодо захисту критичної інфраструктури;

4) створення окремого структурного підрозділу або визначення відповідальної особи за організацію захисту критичної інфраструктури та забезпечення постійного зв'язку з відповідними суб'єктами національної системи захисту критичної інфраструктури;

5) оперативне реагування на протиправні дії, фізичні атаки, спрямовані на відключення або пошкодження роботи операційних систем чи систем забезпечення фізичної безпеки об'єкта критичної інфраструктури;

6) організація заходів з реагування на інциденти, кризові ситуації, а також ліквідації їх наслідків на об'єктах критичної інфраструктури у взаємодії з іншими суб'єктами національної системи захисту критичної інфраструктури;

7) забезпечення відновлення функціонування об'єктів критичної інфраструктури в разі виникнення аварій та інших небезпечних подій, вчинення протиправних дій;

[52] Там само.

8) участь у заходах із захисту повітряного простору над визначеними об’єктами критичної інфраструктури;

9) негайне інформування уповноваженого органу у сфері захисту критичної інфраструктури України, органів Національної поліції України, Служби безпеки України, підрозділів Національної гвардії України, інших державних органів про інциденти, пов’язані з порушеннями систем фізичної безпеки та кібербезпеки, а також інформування Служби безпеки України про загрози та ризики диверсій, терористичних актів, актів кібертероризму проти систем управління, операційних та інших систем об’єктів критичної інфраструктури, надзвичайних ситуацій або інших небезпечних подій на важливих державних об’єктах;

10) забезпечення постійного зв’язку з відповідальними за реагування на протиправні дії та з іншими компетентними організаціями та установами;

11) забезпечення постійної взаємодії з підприємствами, які забезпечують централізоване водопостачання, централізоване водовідведення, постачання теплової енергії, енергопостачання, функціонування електронних комунікаційних мереж, транспортне обслуговування, медичну допомогу, безпеку та інші послуги, від яких залежить процес реагування на кризові ситуації та відновлення функціонування об’єктів критичної інфраструктури;

12) створення і використання необхідних резервів фінансових та матеріальних ресурсів для реагування на кризові ситуації та ліквідації їх наслідків;

13) проведення навчань та тренінгів, підготовка та перевірка персоналу, який відповідає за охорону, безпеку та захист об’єктів критичної інфраструктури;

14) захист інформації про системи управління, зв’язку, фізичну безпеку та кібербезпеку, забезпечення відповідно до встановлених законодавством вимог конфіденційності інформації під час оброблення даних про об’єкти критичної інфраструктури;

15) забезпечення захисту персоналу об’єктів критичної інфраструктури, організація та здійснення евакуаційних заходів у разі виникнення надзвичайних ситуацій.

Крім того, оператори критичної інфраструктури забезпечують розроблення та затвердження у встановленому законодавством порядку вимог щодо організації захисту об’єктів критичної інфраструктури тощо.

Також оператори критичної інфраструктури мають право:

– отримувати в установленому порядку від уповноважених

органів державної влади інформацію про забезпечення безпеки об'єктів критичної інфраструктури;

– самостійно розробляти заходи щодо забезпечення безпеки об'єктів критичної інфраструктури, що не суперечать вимогам цього Закону та ухвалених відповідно до нього нормативно-правових актів;

– отримувати від уповноваженого органу у сфері захисту критичної інфраструктури України консультації щодо застосування законодавства у сфері захисту критичної інфраструктури та вжиття необхідних заходів для захисту критичної інфраструктури.

Водночас зобов'язані оператори критичної інфраструктури:

– забезпечити захист об'єктів критичної інфраструктури;

– невідкладно поінформувати відповідальних суб'єктів національної системи захисту критичної інфраструктури (секторальні та функціональні органи) про інциденти, що сталися на об'єктах критичної інфраструктури, які належать їм на праві власності або на іншій законній підставі;

– завчасно, але не менше ніж за 30 календарних днів до дати зміни стану об'єкта критичної інфраструктури або його частини, інформувати уповноважений орган у сфері захисту критичної інфраструктури України про наміри змінити цільове призначення, режим функціонування чи намір передати права на об'єкт критичної інфраструктури та виконувати надані їм висновки та рекомендації;

– щороку надавати інформацію про виконання повноважень відповідно до Закону України «Про критичну інфраструктуру» за формою, визначеною Кабінетом Міністрів України[53].

Тож розглянемо інші нормативно-правові акти, які регулюють захист та правовий режим об'єктів критичної інфраструктури в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, особливого періоду.

У ст. 4 Закону України «Про правовий режим воєнного стану» від 12.05.2015 № 389-VIII[54] передбачено, що на територіях, де введено воєнний стан, можуть створюватися тимчасові державні органи – військові адміністрації для забезпечення виконання Конституції та законів України, забезпечення разом з військовим командуванням запровадження та здійснення заходів правового режиму воєнного стану, оборони, цивільної оборони, громадської безпеки і порядку, захисту об'єктів критичної інфраструктури, охорони прав, свобод і законних інтересів громадян.

[53] Там само.

[54] Про правовий режим воєнного стану: Закон України від 12.05.2015 № 389-VIII. URL : https://zakon.rada. gov.ua/laws/show/389-19#Text.

Відповідно до п. 7 ст. 4 цього Закону, Генеральний штаб Збройних Сил України спрямовує, координує та контролює діяльність обласних військових адміністрацій з питань оборони, громадської безпеки і порядку, захисту критичної інфраструктури та здійснення заходів правового режиму воєнного стану, а Кабінет Міністрів України в межах своїх повноважень – з інших питань.

Генеральний штаб Збройних Сил України, обласні військові адміністрації (у разі їх створення) спрямовують, координують і контролюють діяльність районних військових адміністрацій з питань оборони, громадської безпеки і порядку, захисту критичної інфраструктури та здійснення заходів правового режиму воєнного стану, а Кабінет Міністрів України та обласні державні адміністрації в межах своїх повноважень – з інших питань.

Статтєю 8 вищезгаданого Закону України передбачає такі заходи правового режиму воєнного стану щодо об'єктів критичної інфраструктури та інших питань:

– п. 1 встановлювати (посилювати) охорону об'єктів критичної інфраструктури та об'єктів, що забезпечують життєдіяльність населення, і вводити особливий режим їх роботи. Порядок встановлення (посилення) охорони таких об'єктів та їх перелік, що із введенням воєнного стану підлягають охороні, а також порядок особливого режиму їх роботи затверджуються Кабінетом Міністрів України;

– п. 2 запроваджувати трудову повинність для працездатних осіб, не залучених до роботи в оборонній сфері та захисту критичної інфраструктури і не забронюваних за підприємствами, установами та організаціями на період дії воєнного стану з метою виконання робіт, що мають оборонний характер, а також ліквідації наслідків надзвичайних ситуацій, які виникли в період дії воєнного стану, та залучати їх в умовах воєнного стану до суспільно корисних робіт, що виконуються для задоволення потреб Збройних Сил України, інших військових формувань, правоохоронних органів і сил цивільного захисту, забезпечення функціонування національної економіки та захисту критичної інфраструктури і не потребують, як правило, спеціальної професійної підготовки осіб. За працівниками, залученими до виконання суспільно корисних робіт, на час виконання таких робіт зберігається попереднє місце роботи (посада). Порядок залучення працездатних осіб в умовах воєнного стану до суспільно корисних робіт та питання їхнього соціального захисту з урахуванням вимог закону визначаються Кабінетом Міністрів України;

– п. 9 порушувати у порядку, визначеному Конституцією та законами України, питання про заборону діяльності політичних партій,

громадських об’єднань, якщо вона спрямована на ліквідацію незалежності України, зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності держави, підрив її безпеки, незаконне захоплення державної влади, пропаганду війни, насильства, на розпалювання міжетнічної, расової, релігійної ворожнечі, посягання на стійкість критичної інфраструктури, права і свободи людини, здоров’я населення.

Тож відповідно до повноважень військові адміністрації населених пунктів на відповідній території здійснюють:

– встановлення посиленої охорони об’єктів критичної інфраструктури та об’єктів, які забезпечують життєдіяльність населення тощо[55].

Наступним нормативним документом щодо правового регулювання захисту та правого режиму об’єктів критичної інфраструктури є Закон України «Про правовий режим надзвичайного стану» від 16.03.2000 № 1550-III. У ньому зазначено, що указом Президента України про введення надзвичайного стану в інтересах національної безпеки та громадського порядку з метою запобігання заворушенням або кримінальним правопорушенням, для охорони здоров’я населення або захисту прав і свобод інших людей на період надзвичайного стану можуть запроваджуватися такі заходи щодо об’єктів критичної інфраструктури та іншого:

– посилення охорони громадського порядку та важливих об’єктів національної економіки та об’єктів критичної інфраструктури[56].

До речі, Закон України «Про функціонування єдиної транспортної системи України в особливий період» від 20.10.1998 № 194-XIV також встановлює особливості захисту та правового режиму об’єктів критичної інфраструктури в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, особливого періоду та встановлює правові та організаційні основи функціонування єдиної транспортної системи України в особливий період, зважаючи на положення законів України «Про мобілізаційну підготовку та мобілізацію», «Про транспорт», «Про оборону України» та інших нормативно-правових актів з питань мобілізаційної підготовки та мобілізації[57].

Однак Закон України «Про оборону України» від 06.12.1991 №

---

[55] Там само.

[56] Про правовий режим надзвичайного стану: Закон України від 16.03.2000 № 1550-III. URL : https://zakon. rada.gov.ua/laws/show/1550-14?find=1&text=критич#w1_1.

[57] Про функціонування єдиної транспортної системи України в особливий період: Закон України від 20.10.1998 № 194-XIV. URL : https://zakon.rada.gov.ua/laws/show/194-14?find=1&text=критич#Text.

1932-XII у ст. 3 зазначає, що підготовка держави до оборони містить у собі таке:

– забезпечення готовності органів державної влади, органів місцевого самоврядування, єдиної державної системи цивільного захисту об'єктів критичної інфраструктури до виконання завдань цивільного захисту в особливий період, зокрема у воєнний час, з урахуванням норм міжнародного гуманітарного права;

– підготовку національної економіки, об'єктів критичної інфраструктури, території, органів державної влади, органів військового управління, органів місцевого самоврядування, а також населення до дій в особливий період.

Кабінет Міністрів України: здійснює загальнодержавні заходи щодо забезпечення живучості важливих об'єктів національної економіки, об'єктів критичної інфраструктури та державного управління у воєнний час.

Щодо Міністерства, то центральні та інші органи виконавчої влади у взаємодії з Міністерством оборони України в межах своїх повноважень:

– узгоджують з Генеральним штабом Збройних Сил України та забезпечують проведення заходів щодо розвитку системи зв'язку, шляхів, транспорту, інших об'єктів критичної інфраструктури і території держави та підготовки своїх галузей до оборони, забезпечують їх територіальну оборону в межах своїх повноважень[58].

[58] Про оборону України: Закон України від 06.12.1991 № 1932-XII. URL : https://zakon.rada.gov.ua/laws/ show/1932-12?find=1&text=критич#w1_1.

Розділ 3
КВАЛІФІКАЦІЯ КРИМІНАЛЬНОГО ПРАВОПОРУШЕННЯ, ПЕРЕДБАЧЕНОГО СТАТТЕЮ 259 «ЗАВІДОМО НЕПРАВДИВЕ ПОВІДОМЛЕННЯ ПРО ЗАГРОЗУ БЕЗПЕЦІ ГРОМАДЯН, ЗНИЩЕННЯ ЧИ ПОШКОДЖЕННЯ ОБ'ЄКТІВ ВЛАСНОСТІ»

Відповідно до єдиних звітів про кримінальні правопорушення обліковано кримінальних правопорушень за ст. 259 КК в 2020 р. – 833, в 2021 р. – 693, в 2022 р. – 1046, в 2023 р. – 1197, за 4 місяці 2024 р. – 547[59]. Як бачимо, з початку агресивного повномасштабного вторгнення рф на територію України кількість правопорушень, передбачених ст. 259 КК, зросла практично вдвічі. У зв'язку з цим виникає питання правильної кваліфікації зазначених кримінальних правопорушень, зокрема в разі їх вчинення щодо об'єктів критичної інфраструктури.

Ст. 259 Кримінального кодексу України містить 2 частини. Відповідно до ч. 1 ст. 259 КК кримінальна відповідальність настає за «завідомо неправдиве повідомлення про підготовку вибуху, підпалу або інших дій, які загрожують загибеллю людей чи іншими тяжкими наслідками».

Родовим об'єктом вказаного злочину є громадська безпека. Під громадською безпекою в кримінальному праві розуміють такий стан суспільства, коли воно перебуває в безпеці.

Безпосередній об'єкт – громадська безпека в частині достовірної інформації про наявні загрози у вигляді вибухів, підпалів тощо. Неправильне визначення безпосереднього об'єкта може призводити до неправильної кваліфікації вчиненого діяння.

> Наприклад, Бабушкінським районним судом м. Дніпропетровська 19 червня 2014 р. було винесено вирок Особі 5. Як було встановлено судом, 19 лютого 2014 року приблизно о 10 год 50 хв ОСОБА_5, перебуваючи в стані алкогольного сп'яніння та знаходячись за місцем свого мешкання, реалізуючи раптово виниклий умисел, по засобах телефонного зв'язку із стаціонарного телефону, що належить йому, здійснив дзвінок операторові і повідомив, що він найближчим часом здійснить вибух в адміністративній будівлі Служби безпеки України, розташованій по вул. Чкалова, буд.

[59] Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. URL : https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

> 23 у м. Дніпропетровську, внаслідок чого була тимчасово порушена нормальна діяльність вищевказаної установи. Дії винного були кваліфіковані за ч. 1 ст. 296 КК «Хуліганство»[60]. На нашу думку, неправильне визначення об'єкта кримінального правопорушення призвело до неправильної кваліфікації і до наступного звільнення винного від кримінальної ідповідальності у зв'язку з дійовим каяттям.

Безпосереднім додатковим об'єктом можуть бути життя та здоров'я осіб.

З об'єктивної сторони вказаний злочин полягає у вчиненні дії, а саме в неправдивому повідомленні:

а) про підготовку вибуху;
б) про підготовку підпалу;
в) про вчинення інших дій, які загрожують загибеллю людей чи іншими тяжкими наслідками.

Фактично законодавець, хоча прямо і не вказує про це, але говорить про неправдиве повідомлення про вчинення терористичного акту.

За особливостями конструкції це формальний склад. Він вважається закінченим з моменту повідомлення хоча б одній особі про неіснуючі загрози (з метою подальшого поширення цього повідомлення). Спосіб доведення повідомлення на кваліфікацію не впливає.

Суб'єктом злочину, передбаченого ст. 259 КК, є фізична осудна особа, яка на момент вчинення цього злочину досягла шістнадцятирічного віку.

Із суб'єктивної сторони злочин, передбачений ст. 259 КК, вчиняється з прямим умислом, винна особа усвідомлює суспільно небезпечний характер свого діяння, усвідомлює, що вона поширює завідомо неправдиве повідомлення про вчинення вибуху, підпалу або інших дій, які загрожують загибеллю людей чи іншими тяжкими наслідками, і бажає так діяти. Мотив та мета на кваліфікацію не впливають.

Законом України «Про внесення змін до статті 259 Кримінального кодексу України щодо посилення відповідальності за завідомо

[60] Вирок Бабушкінського суду м. Дніпропетровська від 19.06.2014 URL : https://reyestr.court.gov.ua/Review/ 39370342.

неправдиве повідомлення про загрозу безпеці громадян»[61] від 2 березня 2021 р. ч. 2 ст. 259 КК була викладена в такій редакції: «Те саме діяння, якщо об'єктами завідомо неправдивого повідомлення стали критично важливі об'єкти інфраструктури або будівлі чи споруди, що забезпечують діяльність органів державної влади, або заклади охорони здоров'я, або заклади освіти або якщо воно спричинило тяжкі наслідки чи вчинене повторно».

Отож кваліфікуючими ознаками злочину, передбаченого ст. 259 КК, є:

1) якщо об'єктами завідомого неправдивого повідомлення стали критично важливі об'єкти інфраструктури або будівлі чи споруди, що забезпечують діяльність органів державної влади, або заклади охорони здоров'я, або заклади освіти;

2) якщо воно спричинило тяжкі наслідки;

3) якщо воно вчинене повторно.

Поняття тяжких наслідків у Кримінальному кодексі України не наводиться. За загальним правилом це оціночне поняття, під яким зазвичай розуміють:

- смерть або тяжкі тілесні пошкодження хоча б 1 особи;
- середньої тяжкості тілесні пошкодження 2 або більше особам;
- інші тяжкі наслідки.

Іншим тяжким наслідком завідомо неправдивого повідомлення про загрозу громадській безпеці є майнова шкода у великих розмірах. Майновою шкодою у великих розмірах треба вважати прямі збитки на суму, яка в триста і більше разів перевищує неоподатковуваний мінімум доходів громадян[62].

Під повторністю треба розуміти вчинення двох або більше злочинів, передбачених ст. 259 КК. При цьому перше діяння кваліфікується за ч. 1 ст. 259 КК (за відсутності кваліфікуючих ознак), а друге – за ч. 2 ст. 259 КК.

> Наприклад, Малиновським районним судом м. Одеси було винесено вирок Особі 4. Як було встановлено судом, 23.04.2017 року о 16 год 49 хв ОСОБА_4, перебуваючи в комп'ютерному клубі «Elite», розташованому за адресою:

[61] Про внесення змін до статті 259 Кримінального кодексу України щодо посилення відповідальності за завідомо неправдиве повідомлення про загрозу безпеці громадян: Закон України. URL : https://zakon.rada. gov.ua/laws/show/1292-20#n5.

[62] Кириченко О. В. Кримінально-правові та кримінологічні аспекти протидії завідомо неправдивим повідомленням про загрозу громадській безпеці: дис. … канд. юрид. наук : 12.00.08. Харків, 2005. 234 с.

м. Одеса, вул. Маршала Малиновського, буд. 33/1, діючи умисно, через неприязні стосунки з керівництвом, з метою порушення громадської безпеки та нормальної діяльності підприємства, із використанням належного йому мобільного телефону марки та моделі «NOKIA 1600» (чорно-сірого кольору,) із СІМ-картки оператора мобільного зв'язку ПрАТ «МТС Україна» здійснив телефонний дзвінок на телефон диспетчерської служби поліції «102», після чого, достовірно знаючи про неправдивість поширюваної ним інформації щодо замінування, усно повідомив оперативного чергового «102» ГУ НП України в Одеській області про те, що магазин заміновано.
Отже, ОСОБА_4 умисно здійснив завідомо неправдиве повідомлення про підготовку вибуху, що загрожує загибеллю людей чи іншими тяжкими наслідками, тобто вчинив кримінальне правопорушення, передбачене ч. 1 ст. 259 КК України.
Крім того, 23.04.2017 року о 19 год 28 хв ОСОБА_4, перебуваючи за своїм місцем проживання, діючи умисно, через неприязні стосунки з сусідами, проживаючими у цьому будинку, діючи повторно, із використанням належного йому мобільного телефону марки та моделі «NOKIA 1600» (чорно-сірого кольору) із СІМ-картки оператора мобільного зв'язку ПрАТ «МТС Україна». здійснив телефонний дзвінок на телефон диспетчерської служби поліції «102», після чого, достовірно знаючи про неправдивість поширюваної ним інформації щодо замінування, усно повідомив оперативного чергового «102» ГУ НП України в Одеській області про те, що житловий багатоквартирний будинок заміновано.
Отже, ОСОБА_4 умисно здійснив завідомо неправдиве повідомлення про підготовку вибуху, що загрожує загибеллю людей чи іншими тяжкими наслідками, вчинене повторно, тобто вчинив кримінальне правопорушення, передбачене ч. 2 ст. 259 КК України[63].

При цьому треба не забувати, що діяння, вчинені з одним умислом, без значного розриву в часі, не утворюють повторності і кваліфікуються за ч. 1 ст. 259 КК.

Відповідно до примітки до ст. 259 КК термін «критично важливі об'єкти інфраструкутри» вживається у значенні, визначеному в Законі

[63] Вирок Малиновського районного суду м. Одеси від 09.05.2023. URL : https://reyestr.court.gov.ua/Review/ 110874502.

України «Про основні засади забезпечення кібербезпеки України»[64].

Відповідно до п. 16 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» критично важливі об'єкти інфраструктури – підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей.

Але Законом України від 16 листопада 2021 р «Про критичну інфраструктуру» було внесено зміни до Закону України «Про основні засади забезпечення кібербезпеки України», відповідно до яких п. 16 ч. 1 виключили, а ч. 2 доповнили реченням такого змісту: «Термін «об'єкт критичної інфраструктури» вживається в цьому Законі у значенні, визначеному Законом України «Про критичну інфраструктуру»«.

Тож під критично важливими об'єктами інфраструктури відповідно до п. 13 ч. 1 ст. 1 Закону України «Про критичну інфраструктуру» треба розуміти об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам[65].

Якщо об'єктами завідомого неправдивого повідомлення стали критично важливі об'єкти інфраструктури незалежно від того, чи вчинено це повідомлення повторно, чи настали внаслідок нього тяжкі наслідки, дії винного кваліфікуються за ч. 2 ст. 259 КК.

> Наприклад, Іллічівським міським судом Одеської області 08 листопада 2023 р. було засуджено за ч. 2 ст. 259 КК Особу 1 за таких обставин: ОСОБА_1, 11 червня 2023 року о 15 год 45 хв, знаходячись за місцем мешкання своєї співмешканки, перебуваючи у стані алкогольного сп'яніння, діючи з прямим умислом, здійснив завідомо неправдиве повідомлення про вибух, з метою порушення громадської безпеки, спокою громадян, нормальної діяльності відділу поліції № 1 б Одеського районного управління поліції № 2 ГУНП в Одеській

[64] Кримінальний кодекс України. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

[65] Про критичну інфраструктуру: Закон України від 16.11.2021 URL : https://zakon.rada.gov.ua/laws/show/ 1882-20#n20.

області (далі ВП № 1 ОРУП № 2 ГУНП в Одеській області), розташованого за адресою: Одеська область, Одеський район, м. Чорноморськ, вул. Хантадзе, 15, який відповідно до статті 19 Закону України «Про критичну інфраструктуру», пунктів 4-7 Порядку віднесення об'єктів до критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 09.10.2020 № 1109 (у редакції постанови Кабінету Міністрів України від 16.12.2022 № 1384), наказу Міністерства внутрішніх справ України від 23.03.2023 № 236 ДСК «Про затвердження Переліку об'єктів критичної інфраструктури сектору громадської безпеки, є критично важливим об'єктом інфраструктури, що забезпечує діяльність органу державної влади, усвідомлюючи, що його завідомо неправдиве повідомлення викличе обстановку страху у населення та інших жителів м. Чорноморська Одеської області, порушить громадське безпеку, із використанням належного йому мобільного телефону марки «Xiaomi», моделі «Redmi 9-C», в корпусі чорного кольору, із сім-карткою оператора «Лайфселл», здійснив телефонний дзвінок на спецлінію за номером абонента «102» та після з'єднання, в телефонному режимі, повідомив оперативного чергового спецлінії «102» ГУНП в Одеській області про те, що «Чорноморське відділення (ВП № 1 ОРУП № 2 ГУНП в Одеській області) заміноване бомбою, скоріше!», після чого поклав слухавку.

Внаслідок злочинних дій ОСОБА_1, пов'язаних із неправдивим повідомленням щодо замінування вищевказаної адміністративної будівлі, яка є критично важливим об'єктом інфраструктури, що забезпечує діяльність органу державної влади, слідчою-оперативною групою ВП № 1 ОРУП № 2 ГУНП в Одеській області були проведені слідчі та оперативно-розшукові заходи з пошуку можливого замінування чи вибухового пристрою. За наслідками відпрацювання завідомо неправдивого повідомлення, і закінченню проведення огляду місця події вибухових пристроїв чи небезпечних речей не виявлено. Тим самим ОСОБА_1 здійснив завідомо неправдиве повідомлення про підготовку вибуху, який загрожує загибеллю людей та іншими тяжкими наслідками, порушив громадську безпеку та спокій осіб, які перебували у ВП № 1 ОРУП № 2 ГУНП Одеській області, що розташований за адресою: Одеська область, Одеський район, Чорноморськ, вул. Хантадзе, 15, тимчасово припинив нормальну діяльність роботи вказаної адміністративної будівлі, яка є критично важливим об'єктом інфраструктури, що забезпечує діяльність органу державної влади, внаслідок чого були задіяні сили правоохоронних

органів для перевірки неправдивого повідомлення та пошуки вибухового пристрою.
Отже, ОСОБА_1 вчинив кримінальне правопорушення, передбачене частиною 2 статті 259 Кримінального кодексу України, за кваліфікуючим ознаками: завідоме неправдиве повідомлення про підготовку вибуху, який загрожує загибеллю людей та іншими тяжкими наслідками, об'єктом якого став критично важливий об'єкт інфраструктури, що забезпечує діяльність органу державної влади[66].

Окремо в ч. 2 ст. 259 КК законодавець виділив будівлі чи споруди, що забезпечують діяльність органів державної влади. Під органом державної влади зазвичай розуміють органи, яким надані владні повноваження та які діють від імені держави як на всій території держави, так і в окремих її адміністративно-територіальних одиницях.

Наприклад Новоград-Волинським міськрайонним судом Житомирської області 18 січня 2024 р. було засуджено Особу 4 за таких обставин. 18.10.2023 приблизно 15 год у ОСОБА_4, який перебував на території автовокзалу, що розташований по вул. Шевченка 45 в м. Звягель Житомирської області, виник злочинний умисел, спрямований на завідомо неправдиве повідомлення правоохоронним органам про підготовку вибуху у будівлі Звягельської міської ради Житомирської області (далі по тексту – Міська рада), достовірно знаючи при цьому про неправдивий характер поширюваної ним інформації та розуміючи, що таке повідомлення викличе обстановку страху та паніки у населення, порушить їх нормальний ритм життя та громадський спокій.
З метою реалізації свого злочинного умислу, усвідомлюючи суспільно небезпечний характер своїх дій та настання суспільно небезпечних наслідків у вигляді шкоди громадській безпеці, а також бажаючи їх настання, 18.10.2023 о 15:04 год ОСОБА_4, перебуваючи на території автовокзалу, за допомогою власного мобільного телефону марки «Realme C21», обладнаного сім-картками оператора мобільного зв'язку «Київстар», зателефонував на спецлінію «102» ГУНП в Житомирській області. Далі він повідомив інформацію про встановлення бойового припасу – гранати та підготовку вибуху у будівлі Міської ради, розташованої по вул. Шевченка, 16 в м. Звягель, Житомирської області, в якій також розміщені приміщення Звягельської районної військової адміністрації

[66] Вирок Іллічівського міського суду Одеської області від 08.11.2023. URL : https://reyestr.court.gov.ua/ Review/114757584.

Житомирської області, які згідно з приміткою до ст. 259 КК України є критично важливими об'єктами інфраструктури та будівлею, що забезпечує діяльність органів державної влади, що призвело до породження паніки та порушення нормального ритму життя населення, внесення дезорганізації у функціонування державних установ, а також до безпідставного відволікання сил і засобів спеціальних служб для перевірки вказаного повідомлення.
За результатами перевірки повідомлення ОСОБА_4 про підготовку вибуху в приміщенні вищевказаної будівлі вибухонебезпечних предметів не виявлено, що підтверджує неправдивість повідомленої останнім інформації.
Отже, суд кваліфікував дії ОСОБА_4 за ч. 2 ст. 259 КК України, які виразились у завідомо неправдивому повідомленні про підготовку вибуху, який загрожує загибеллю людей чи іншими тяжкими наслідками, об'єктом якого став критично важливий об'єкт інфраструктури та будівля, що забезпечує діяльність органів державної влади[67].

Заклад охорони здоров'я – юридична особа будь-якої форми власності та організаційно-правової форми або її відокремлений підрозділ, що забезпечує медичне обслуговування населення на основі відповідної ліцензії та професійної діяльності медичних (фармацевтичних) працівників і фахівців з реабілітації. (ч. 1 ст. 3 Закону України «Основи законодавства України про охорону здоров'я»)[68].

Наприклад, Орджонікідзевським районним судом м. Запоріжжя 01 липня 2022 р. було засуджено Особу 4 за таких обставин. 13.02.2022, приблизно о 01 год 17 хв, ОСОБА_4, перебуваючи у стані алкогольного сп'яніння, діючи умисно, усвідомлюючи суспільно-небезпечний характер своїх дій, передбачаючи суспільно-небезпечні наслідки і бажаючи їх настання, з особистих спонукань вирішив зателефонувати оператору «102» із завідомо неправдивим повідомленням про замінування закладу охорони здоров'я комунального некомерційного підприємства «Міська лікарня екстреної та швидкої медичної допомоги» Запорізької міської ради, розташованого за адресою: м. Запоріжжя, вул. Перемоги, буд. 80.
Реалізуючи свій злочинний умисел безпосередньо після його

[67] Вирок Новоград-Волинського міськрайонного суду Житомирської області від 18.01.2024. URL : https://reyestr.court.gov.ua/Review/116384203.

[68] Основи законодавства України про охорону здоров'я: Закон України від 19.11.1992 в редакції від 19.04.2024. URL : https://zakon.rada.gov.ua/laws/show/2801-12#Text.

> виникнення, ОСОБА_6 4, перебуваючи за адресою: АДРЕСА_2, шляхом здійснення телефонного дзвінка з власного мобільного телефону «Meizu M5» зі встановленою сім-картою мобільного оператора «Київстар» оператору «102», достовірно знаючи, що поширювана ним інформація є неправдивою, розуміючи, що таке повідомлення породить паніку та страх серед населення, а також порушить громадську безпеку, повідомив завідомо неправдиву інформацію про замінування та вибух комунального некомерційного підприємства «Міська лікарня екстреної та швидкої медичної допомоги» Запорізької міської ради, що розташована за адресою: місто Запоріжжя, вул. Перемоги буд. 80, який загрожує загибеллю людей та іншими тяжкими наслідками, що призвело до безпідставного відволікання сил і засобів спеціальних служб для перевірки вказаного повідомлення.
> Умисні дії ОСОБА_4 було кваліфіковано за ч. 2 ст. 259 КК України, як завідомо неправдиве повідомлення про вчинення вибуху, який загрожує загибеллю людей чи іншими тяжкими наслідками, якщо об'єктом завідомо неправдивого повідомлення став заклад охорони здоров'я[69].

І останнім об'єктом завідомо неправдивого повідомлення, передбаченого ч. 2 ст. 259 КК є заклади освіти. Відповідно до п. 6 ч. 1 ст. 1 Закону України «Про освіту» заклад освіти – це юридична особа публічного чи приватного права, основним видом діяльності якої є освітня діяльність[70].

> Наприклад, 26 серпня 2021 р. Володимир-Волинським міським судом Волинської області було засуджено Особу 4 за таких обставин. 29.05.2021 о 19 год 18 хв військовослужбовець військової частини старший солдат ОСОБА_4, знаходячись в позаслужбовий час у м. Володимир-Волинський Волинської області неподалік закладу освіти Володимир-Волинської загальноосвітньої школи І-ІІІ ступенів № 2 Володимир-Волинської міської ради Волинської області, розташованої за адресою: вул. Котляревського, 2, м. Володимир-Волинський Волинської області, будучи в стані алкогольного сп'яніння, діючи умисно, усвідомлюючи суспільно небезпечний характер своїх дій та передбачаючи настання суспільно небезпечних

[69] Вирок Орджонікідзевського районного суду м. Запоріжжя від 01.07.2022. URL : https://reyestr.court.gov. ua/Review/105030909.

[70] Про освіту: Закон України від 05.09.2017. URL : https://zakon.rada.gov.ua/laws/show/2145-19#Text.

наслідків у вигляді шкоди громадській безпеці, реалізуючи раптово виниклий злочинний умисел, спрямований на завідомо неправдиве повідомлення про підготовку вибуху або інших дій, які загрожують загибеллю людей чи іншими тяжкими наслідками, достовірно знаючи про неправдивий характер поширюваної ним інформації та розуміючи, що таке повідомлення створить обстановку загального страху і невпевненості, паніку в населення, порушить громадську безпеку, нормальний ритм життя та спокій населення, нехтуючи вимогами законодавства, здійснив з власного мобільного телефону марки «XIAOMI», обладнаного сім-карткою оператора стільникового зв'язку «LIFECELL» телефонний дзвінок на лінію екстреного виклику служби «102» Управління організаційно-аналітичного забезпечення та оперативного реагування Головного управління Національної поліції у Волинській області, під час якого повідомив оператору комп'ютерного набору відділу служби Управління організаційно-аналітичного забезпечення та оперативного реагування Головного управління Національної поліції у Волинській області завідомо неправдиву інформацію про підготовку вибуху або інших дій, які загрожують загибеллю людей чи іншими тяжкими наслідками, а саме про своє бажання та наміри здійснити вибух приміщення закладу освіти, розташованого за адресою: вул. Котляревського, 2, м. Володимир-Волинський Волинської області, з використанням ручного протитанкового гранатомета, після чого затриманий поліцейськими, чим вчинив завідомо неправдиве повідомлення про підготовку вибуху або інших дій, які загрожують загибеллю людей чи іншими тяжкими наслідками, якщо об'єктом завідомо неправдивого повідомлення стали заклади освіти. Суд визнав Особу 4 винуватим у вчиненні злочину, передбаченого ч. 2 ст. 259 КК України[71].

[71] Вирок Володимир-Волинського міського суду Волинської області від 26.08.2021. URL : https://reyestr. court.gov.ua/Review/99182601.

РОЗДІЛ 4
КВАЛІФІКАЦІЯ КРИМІНАЛЬНОГО ПРАВОПОРУШЕННЯ, ПЕРЕДБАЧЕНОГО СТАТТЕЮ 360 КК «УМИСНЕ ПОШКОДЖЕННЯ АБО РУЙНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ»

Відповідно до єдиних звітів про кримінальні правопорушення обліковано кримінальних правопорушень за ст. 360 КК в 2020 р. – 623 (з них ч. 1 ст. 360 – 155, ч. 2, 3 ст. 360 – 468), в 2021 р. – 676 (з них ч. 1 ст. 360 – 172, ч. 2, 3 ст. 360 – 504), в 2022 р. – 310 (з них ч. 1 ст. 360 – 146, ч. 2, 3 ст. 360 – 164), в 2023 р. – 502 (з них ч. 1 ст. 360 – 144, ч. 2, 3 ст. 360 – 358), за 4 місяці 2024 р. – 155 (з них ч. 1 ст. 360 – 71, ч. 2, 3 ст. 360 – 84)[72]. Як бачимо, кількість облікованих кримінальних правопорушень за ч. 2, 3 ст. 360 КК в середньому вдвічі перевищує кількість облікованих кримінальних правопорушень за ч. 1 ст. 360 КК.

З ухваленням чинного Кримінального кодексу України в 2001 р. ст. 360 КК отримала назву «Умисне пошкодження ліній зв'язку» та містила 1 частину «Умисне пошкодження кабельної, радіорелейної, повітряної лінії зв'язку, проводового мовлення або споруд чи обладнання, які входять до їх складу, якщо воно спричинило тимчасове припинення зв'язку».

Законом України «Про внесення змін до деяких законодавчих актів України щодо посилення захисту телекомунікаційних мереж» ст. 360 КК «Умисне пошкодження або руйнування телекомунікаційної мережі» викладена в новій редакції та отримала 3 частини.

Як зазначалось в пояснювальній записці до проєкту Закону України «Про внесення змін до деяких законодавчих актів України (щодо посилення захисту телекомунікаційних мереж)», причинами внесення змін до ст. 360 КК є збільшення кількості випадків знищення та руйнування телекомунікаційних мереж, необхідність посилення заходів по боротьбі з цим негативним явищем, недосконаліть диспозиції ст. 360 КК в редакції 2001 р. та невідповідність її чинному законодавству, а також відмежування від ст. 147 КУпАП.

Відповідно до ч. 1 ст. 360 КК кримінальна відповідальність настає за «умисне пошкодження або руйнування телекомунікаційної мережі чи технічних засобів телекомунікації, чи споруд електрозв'язку, що входять до складу телекомунікаційної мережі, якщо такі дії спричинили припинення надання телекомунікаційних послуг».

[72] Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. URL : https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

Родовим об'єктом вказаного кримінального правопорушення є авторитет органів державної влади, органів місцевого самоврядування, об'єднань громадян та суспільні відносини у сфері захисту журналістів.

Безпосередній об'єкт – нормальна робота телекомунікаційних мереж України. Під телекомунаційним мережами треба розуміти комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням (ч. 1 ст. 1 Закону України «Про телекомунікації»)[73].

Але Законом України «Про електронні комунікації» від 16 грудня 2020 р. Закон України «Про телекомунікації» визнано таким, що втратив чинність[74]. Сам Закон України «Про електронні комунікації» не містить роз'яснення терміна «телекомунікаційні мережі». У прикінцевих та перехідних положеннях зазначеного Закону внесено зміни в Кодекс цивільного захисту України, у Законі України »Про Національну систему конфіденційного зв'язку», у Переліку документів дозвільного характеру у сфері господарської діяльності, затвердженому Законом України «Про Перелік документів дозвільного характеру у сфері господарської діяльності» тощо термін «телекомунікаційни мережі» замінено терміном «електронні комунікаційні мережі». Водночас у Кримінальний кодекс України відповідні зміни так і не було внесено. Це може викликати проблеми в застосуванні ст. 360 КК України.

Вважаємо, що з 01.01.2022 р (з дати набрання чинності Закону України «Про електронні комунікації») під телекомунікаційними мережами треба розуміти електронні комунікаційні мережі.

Відповідно до п. 25 ч. 1 ст. 2 Закону України «Про електронні комунікації» електронна комунікаційна мережа – це комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг.

Безпосереднім додатковим об'єктом є право власності.

Предмет кримінального правопорушення:

– телекомунікаційні мережі (електронні комунікаційні мережі);

– технічні засоби телекомунікації (технічні засоби електронних комунікацій);

– споруди електрозв'язку, що входять до складу

[73] Про телекомунікації: Закон України від 18.11.2003 (втратив чинність). URL : https://zakon.rada.gov.ua/ laws/show/1280-15#Text.

[74] Про електронні комунікації: Закон України від 16.12.2020 URL : https://zakon.rada.gov.ua/laws/show/ 1089-20#n2246.

телекомунікаційної мережі.

Під технічними засобами телекомунікацій (технічними засобами електронних комунікацій) відповідно до п. 130 ч. 1 ст. 2 Закону України «Про електронні комунікації» треба розуміти обладнання, зокрема із встановленим програмним забезпеченням, станційні та лінійні споруди, призначені для організації електронних комунікаційних мереж.

Під спорудами електрозв'язку, що входять до складу телекомунікаційної мережі відповідно до ч. 1 ст. 1 Закону України «Про телекомунікації» треба розуміти будівлі, вежі, антени, що використовуються для організації електрозв'язку.

З об'єктивної сторони кримінальне правопорушення, передбачене ст. 360 КК, повинно містити:

1. Діяння у вигляді пошкодження або руйнування вищевказаних предметів.

2. Наслідок у вигляді припинення надання телекомунікаційних послуг.

3. Причинний зв'язок між діянням та наслідком.

Під пошкодженням у кримінальному праві України розуміють погіршення якості, зменшення цінності речі або приведення її на якийсь час у не придатний до використання за цільовим призначенням стан[75]. У контексті ст. 360 КК під пошкодженням телекомунікаційних мереж треба розуміти приведення її на якийсь час у не придатний до використання за цільовим призначенням стан, а під руйнуванням – приведення телекомунікаційних мереж у повну непридатність до використання за цільовим призначенням, фізичне знищення телекомунікаційних мереж при неможливості їх відновлення.

Кримінальне правопорушення вважається закінченим з моменту настання суспільно-небезпечних наслідків у вигляді припинення надання телекомунікаційних послуг.

Суб'єкт кримінального правопорушення – фізична осудна особа віком від 16 років.

Суб'єктивна сторона кримінального правопорушення, передбаченого ст. 360 КК, характеризується умисною формою вини, у вигляді як прямого, так і непрямого умислу, а саме винна особа усвідомлює суспільно небезпечний характер свого діяння, усвідомлює, що вона пошкоджує або руйнує телекомунікаційні мережі чи технічні засоби телекомунікації, чи споруди електрозв'язку, що входять до

[75] Про судову практику в справах про знищення та пошкодження державного чи колективного майна шляхом підпалу або внаслідок порушення встановлених законодавством вимог пожежної безпеки: Постанова Пленуму Верховного Суду України № 4 від 02.07.1976 URL : https://zakon.rada.gov.ua/laws/ show/v0004700-76#Text.

складу телекомунікаційної мережі, передбачає настання наслідків у вигляді припинення надання телекомунікаційних послуг і бажає настання таких наслідків, або не бажає, але свідомо припускає їх.

Треба відмітити, що пошкодження предметів, вказаних у диспозиції ст. 360, поєднане з незаконним викраденням їх складових, потребує додаткової кваліфікації за статтями, що передбачають кримінальну відповідальність за відповідні кримінальні правопорушення проти власності.

> Наприклад, 12 грудня 2023 р. Голосіївським районним судом м. Києва було засуджено Особу 5 за таких обставин. У невстановлений досудовим розслідуванням час, але не пізніше 04 год 20 січня 2023 року, ОСОБА_5, маючи злочинний умисел, спрямований на таємне викрадення чужого майна, прибув до оглядових колодязів кабельної каналізації № 257-864а та № 257-1334, що знаходяться поблизу буд. № 14 по вул. Кустанайській у м. Києві.
>
> Реалізуючи свій злочинний умисел, спрямований на таємне викрадення чужого майна, ОСОБА_5, усвідомлюючи суспільно небезпечний характер своїх дій, передбачаючи їх суспільно небезпечні наслідки та бажаючи їх настання, діючи таємно, умисно, в умовах воєнного стану, з корисливих мотивів та мети, шляхом відкриття люків оглядових колодязів кабельної каналізації № 257-864а та № 257-1334, проник до підземної кабельної каналізації (сховища для зберігання кабелів діючих ліній зв'язку) АТ «Укртелеком», де з використанням заздалегідь підготовленого знаряддя скоєння кримінального правопорушення демонтував відрізок кабелю зв'язку марки ТПП 100х2х0,4 (інв. № 10110 Цех мережі доступу № 1 Київської міської філії АТ «Укртелеком», введений в експлуатацію у 2005 році), довжиною 71 м, який був прокладений між оглядовими колодязями кабельної каналізації № 257-864а та № 257-1334 і належав АТ «Укртелеком».
>
> Внаслідок пошкодження кабельної лінії зв'язку 17 абонентів з числа жителів м. Києва залишились без телефонного зв'язку.
>
> Крім того, у невстановлений досудовим розслідуванням час, але не пізніше 05 год, 30 січня 2023 року, ОСОБА_5, маючи злочинний умисел, спрямований на таємне викрадення чужого майна, прибув до оглядових колодязів кабельної каналізації № 257-1839 та № 257-1842, що знаходяться поблизу буд. № 35 «Б» по вул. Деміївській у м. Києві.
>
> Реалізуючи свій злочинний умисел, спрямований на таємне викрадення чужого майна, ОСОБА_5, усвідомлюючи суспільно

небезпечний характер своїх дій, передбачаючи їх суспільно небезпечні наслідки та бажаючи їх настання, діючи таємно, умисно, повторно, в умовах воєнного стану, з корисливих мотивів та мети, шляхом відкриття люків оглядових колодязів кабельної каналізації № 257-1839 та № 257-1842, проник до підземної кабельної каналізації (сховища для зберігання кабелів діючих ліній зв'язку) АТ «Укртелеком», де з використанням заздалегідь підготовленого знаряддя скоєння кримінального правопорушення демонтував відрізок кабелю зв'язку марки ТПП 100х2х0,4 (інв. № 10110 Цех мережі доступу № 1 Київської міської філії АТ «Укртелеком», введений в експлуатацію у 2005 році), довжиною 54 м, та відрізок кабелю зв'язку марки ТПП 50х2х0,4 (інв. № 10110 Цех мережі доступу № 1 Київської міської філії АТ «Укртелеком», введений в експлуатацію у 2005 році), довжиною 54 м, які були прокладені між оглядовими колодязями кабельної каналізації № 257-1839 та № 257-1842 і належали АТ «Укртелеком».

Внаслідок пошкодження кабельної лінії зв'язку, вчиненому повторно, 54 абоненти з числа жителів м. Києва залишились без телефонного зв'язку.

ОСОБА_5 була визнана судом винуватою, а її дії були кваліфіковані за ч. 4 ст. 185 КК України, – таємне викрадення чужого майна, вчинене повторно, поєднане з проникненням у сховище, вчинене в умовах воєнного стану, за ч. 1 ст. 360 КК України, – умисне пошкодження телекомунікаційної мережі, що спричинило припинення надання телекомунікаційних послуг, за ч. 2 ст. 360 КК України, – умисне пошкодження телекомунікаційної мережі, що спричинило припинення надання телекомунікаційних послуг, вчинене повторно[76].

Кваліфікуючими ознаками, передбаченими ч. 2 ст. 360 КК, є вчинення цього діяння:

- повторно;
- за попередньою змовою групою осіб;
- загальнонебезпечним способом.

Під повторністю треба розуміти вчинення двох або більше кримінальних правопорушень, передбачених ст. 360 КК. Перше діяння кваліфікується за ч. 1 ст. 360 КК (за відсутності інших обтяжливих обставин), друге – кваліфікується за ч. 2 ст. 360 КК, як вчинене повторно (за відсутності інших обтяжливих обставин). Інколи

[76] Вирок Голосіївського районного суду м. Києва від 12.12.2023 URL : https://reyestr.court.gov.ua/Review/ 115695145.

правоохоронні органи можуть допускати помилки у кваліфікації повторності кримінального правопорушення, передбаченого ст. 360 КК.

Наприклад, Суворовським районним судом м. Одеси 22.05.2024 р. було засуджено Особу 4 за таких обставин.

10.08.2021 року приблизно о 04 год, ОСОБА_4 підійшов до колодязя кабельної каналізації, де за допомогою гострого предмета пошкодив оптичний кабель зв'язку ОКЛБГ-3-ДА12-2х4Е-0,40Ф3,5/0,30Н19-8/0, що призвело до тимчасового припинення зв'язку, завдавши АТ «Укртелеком» майнової шкоди на проведення відновлювальних робіт у розмірі 20034 гривні 02 копійки.

Крім того, 10.08.2021 року приблизно о 04 год 56 хв ОСОБА_4 підійшов до колодязя кабельної каналізації, де за допомогою гострого предмета пошкодив оптичний кабель зв'язку ОКЛБг-3-ДА(3,5)2П-8х12Е1-0,36Ф3,5/0,22Н18-96/0, що призвело до тимчасового припинення зв'язку, завдавши АТ «Укртранснафта» майнової шкоди на проведення відновлювальних робіт у розмірі 2131 гривня 92 копійки.

Крім того, 11.08.2021 року приблизно о 04 год ОСОБА_4 підійшов до колодязя кабельної каналізації, де за допомогою гострого предмета пошкодив оптичний кабель зв'язку ОКЛБГ-3-ДА-12-2х4Е-0,40Ф3,5/0,30Н19-8/0, що призвело до тимчасового припинення зв'язку, завдавши АТ «Укртранснафта» майнової шкоди на проведення відновлювальних робіт у розмірі 15032 гривень 31 копійка.

Крім того, 17.02.2022 року, приблизно о 15 год 40 хв ОСОБА_4 шляхом відчинення люку проник у кабельний колодязь, звідки таємно викрав два відрізки мідного кабелю марки ТПП100х2х0,4 загальною довжиною 44 м, вартість якого становить 5146 гривень 24 копійки.

У подальшому ОСОБА_4 із викраденим майном залишив місце вчинення кримінального правопорушення, розпорядившись ним на власний розсуд, заподіявши ПАТ «Укртелеком» на загальну суму 5146 гривень 24 копійки.

У діях ОСОБА_4 по першому епізоду, а саме по епізоду від 10.08.2021 року о 04 год, прокурор вбачає ознаки кримінального правопорушення, передбаченого ч. 2 ст. 360 КК України, які органом досудового слідства кваліфіковані, як умисне пошкодження телекомунікаційної мережі, що входять до складу телекомунікаційної мережі, що спричинили припинення надання телекомунікаційних послуг, вчинений повторно.

Однак суд вважає за необхідне виключити з інкримінованого

ОСОБА_4 обвинувачення по першому епізоду пошкодження кабелю кваліфікаційну ознаку – «вчиненого повторно», як надмірно застосовану, інкримінування особі ознаки повторності у цьому конкретному випадку є зайвим, оскільки судом встановлено, що фактично, спочатку ОСОБА_4 пошкодив перший кабель, та раніше за аналогічні правопорушення не притягувався, тому підстав для інкримінування обвинуваченому цієї кваліфікуючої ознаки за першим епізодом немає.
Зважаючи на все вищевказане, суд кваліфікував дії ОСОБА_4 за ч. 1 ст. 360 КК України за ознаками: умисне пошкодження телекомунікаційної мережі, що входять до складу телекомунікаційної мережі, що спричинили припинення надання телекомунікаційних послуг (1-й епізод); за ч. 2 ст. 360 КК України за ознаками: умисне пошкодження телекомунікаційної мережі, що входять до складу телекомунікаційної мережі, що спричинили припинення надання телекомунікаційних послуг, вчинений повторно (2-й епізод), за ч. 3 ст. 185 КК України за ознаками: таємне викрадення чужого майна (крадіжка), поєднана з проникненням у сховище, вчинена повторно (3-й епізод, він був раніше судимий)[77].

За попередньою змовою групою осіб означає, що це кримінальне правопорушення спільно вчинили декілька осіб (дві або більше), які заздалегідь, тобто до початку кримінального правопорушення, домовилися про спільне його вчинення.

Наприклад, Київським районним судом м. Одеси 10.02.2023 р. було засуджено Особу 4 та Особу 5 за таких обставин.
05.11.2022 року о 21 год 20 хв в м. Одеса по проспекту Небесної Сотні, біля будинку № 9 + 10 метрів, ОСОБА_4 та ОСОБА_5, діючи за попередньою змовою групою осіб, умисно, скориставшись тим, що за їх діями ніхто не спостерігає, ОСОБА_5 почав спостерігати за відсутністю сторонніх осіб, а ОСОБА_4 шляхом власної сили відкрив кришку люку кабельної каналізації та проник до вказаного приміщення, після чого, шляхом канцелярського ножа, пошкодив кабелі зв'язку марки ТПП 200х2х0,4, довжиною по 126 м, всього 252 м, та марки ТПП 100х2х0,4, довжиною 126 м, належний АТ «Укртелеком», вартість одного метра кабелю зв'язку ТПП 100х2х0,4 становить 189,56 гривень, а вартість

[77] Вирок Суворовського районного суду м. Одеси від 22.05.2024. URL : https://reyestr.court.gov.ua/Review/ 119239171.

одного метра кабелю зв'язку ТПП 200х2х0,4 становить 379,40 гривень, що спричинило АТ «Укртелеком», матеріальну шкоду на загальну суму 99579,06 гривень та припинення надання телекомунікаційних послуг 6 абонентам.

Після чого ОСОБА_4 разом з ОСОБА_5 було затримано працівниками ООО «Охорона сервіс» на місці вчинення кримінального правопорушення, разом з пошкодженим майном.

За таких обставин своїми умисними діями ОСОБА_4 та ОСОБА_5 вчинили кримінальне правопорушення, передбачене ч. 2 ст. 360 КК України, за кваліфікуючими ознаками умисне пошкодження телекомунікаційної мережі, що спричинило припинення надання телекомунікаційних послуг, вчинене за попередньою змовою групою осіб[78].

Під загальнонебезпечним способом розуміють спосіб, який створює реальну загрозу заподіяння шкоди або фактично її заподіює не лише об'єктові, на який посягає винний, а й іншим об'єктам. Такими способами, зокрема, можуть бути підпали, вибухи тощо[79].

Особливо кваліфікуючими ознаками ч. 3 ст. 360 КК є вчинення цих дій:

1) якщо вони заподіяли майнову шкоду у великому розмірі;
2) якщо вони спричинили тяжкі наслідки.

Під майновою шкодою у великому розмірі треба розуміти шкоду, якщо її розмір у тисячу і більше разів перевищує неоподатковуваний мінімум доходів громадян (ч. 1 Примітки до ст. 360 КК).

Під тяжкими наслідками треба розуміти спричинення припинення надання телекомунікаційних послуг на критично важливі об'єкти інфраструктури (ч. 2 Примітки до ст. 360 КК).

Враховуючи, що до об'єктів критичної інфраструктури відносять об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам то умисне пошкодження або руйнування телекомунікаційної мережі чи технічних засобів телекомунікації, чи споруд електрозв'язку, що входять до складу телекомунікаційної мережі, що спричинило припинення надання телекомунікаційних послуг об'єктів оборони чи національної безпеки, вчинені з метою ослаблення держави, кваліфікуються за сукупністю кримінальних правопорушень, передбачених ч. 3 ст. 360 КК та ст. 113 КК.

---

[78] Вирок Київського районного суду м. Одеси від 10.02.2023. URL : https://reyestr.court.gov.ua/Review/ 108903689.

[79] Юріков О. О. Кримінальна відповідальність за умисне пошкодження або руйнування телекомунікаційної мережі: дис. … д-ра філософії за спец. 081 – Право. Київ, 2021. 311 с.

Якщо особа пошкоджує або руйнує телекомунікаційні мережі чи технічні засоби телекомунікації, чи споруди електрозв'язку, що входять до складу телекомунікаційної мережі, що належать об'єктам оборони України (у разі визнання їх критично важливими об'єктами інфраструктури), і умислом винної особи охоплено суспільно небезпечні наслідки у вигляді припинення надання телекомунікаційних послуг, то такі дії підлягають кваліфікації за сукупністю кримінальних правопорушень, передбачених ч. 3 ст. 360 КК та 411 КК України.

У разі, коли особа пошкодила або зруйнувала телекомунікаційні мережі чи технічні засоби телекомунікації, чи споруди електрозв'язку, що входять до складу телекомунікаційної мережі, спричинивши припинення надання телекомунікаційних послуг на критично важливі об'єкти інфраструктури і при цьому переслідувала ще й корисливий мотив та мету збагачення, то дії винного кваліфікуються за сукупністю ч. 3 ст. 360 КК та відповідних частин та статей корисливих кримінальних правопорушень проти власності (ст. 185–187 КК, ст. 189–191 КК).

Враховуючи, що суб'єктивна сторона ст. 360 КК передбачає виключно умисну форму вини, то пошкодження або руйнування телекомунікаційної мережі чи технічних засобів телекомунікації, чи споруд електрозв'язку, що входять до складу телекомунікаційної мережі зі спричиненням припинення надання телекомунікаційних послуг на критично важливі об'єкти інфраструктури, вчинене з необережності, може кваліфікуватися за ст. 196 КК у разі нанесення тяжких тілесних ушкоджень або загибелі хоча б однієї людини.

ВИСНОВКИ

За результатами виконаного дослідження варто зазначити таке:

1. Захист об’єктів критичної інфраструктури в умовах воєнного стану залишається пріоритетним завданням сил безпеки і оборони України, зокрема Національної поліції України, Національної гвардії України, Державної служби з надзвичайних ситуацій, Служби безпеки України.

2. У сучасних умовах збройної агресії російської федерації проти України наявна чинна законодавча база з питань забезпечення безпеки функціонування об’єктів критичної інфраструктури є актуальною та розгалуженою, але такою, що потребує постійного моніторингу у світлі постійних змін впливу як зовнішніх, так і внутрішніх загроз військового і невійськового характеру та внесення відповідних змін та доповнень.

3. Порівняльне дослідження нормативного визначення поняття «об’єкти критичної інфраструктури» у чинному національному законодавстві та законодавстві окремих країн Європейського Союзу показало повні відмінності, які заслуговують уваги. Зокрема, в національному законодавстві визначення «об’єкти критичної інфраструктури» містить об’єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам. Законодавча база європейських країн у сфері захисту критичної інфраструктури містить різний перелік життєво важливих (критичних) інфраструктур (об’єктів). Він визначається відповідно до їхніх традицій, суспільних та політичних переконань, а також географічних та історичних особливостей кожної держави.

Важливою частиною критичної інфраструктури є їх інформаційна складова – критична інформаційна інфраструктура. Зважаючи на національний та закордонний досвід, змісту у визначенні поняття «об’єкти критичної інфраструктури» до таких об’єктів у широкому значенні належать: урядування та надання найважливіших публічних (адміністративних) послуг; енергозабезпечення (зокрема постачання теплової енергії); водопостачання та водовідведення; продовольче забезпечення; охорона здоров’я; фармацевтична промисловість; виготовлення вакцин, стале функціонування біолабораторій;

інформаційні послуги; електронні комунікації; фінансові послуги; транспортне забезпечення; оборона, державна безпека; правопорядок, здійснення правосуддя, тримання під вартою; цивільний захист населення та територій, служби порятунку; космічна діяльність, космічні технології та послуги; хімічна промисловість; дослідницька діяльність.

4. Щодо національно-правового механізму регулювання захисту та правового режиму об'єктів критичної інфраструктури в умовах надзвичайних ситуацій, надзвичайного та воєнного станів, особливого періоду, то він розроблений на державному рівні.

Зокрема, Закон України «Про критичну інфраструктуру» регулює відносини у сфері функціонування та захисту критичної інфраструктури в цілому та її об'єктів у мирний час. Закони України «Про правовий режим воєнного стану», «Про правовий режим надзвичайного стану», «Про функціонування єдиної транспортної системи України в особливий період» та «Про оборону України» визначають особливості захисту та правового режиму об'єктів критичної інфраструктури в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, а також в особливий період. Окремим законом регулюються відносини у сфері кіберзахисту та кібербезпеки об'єктів критичної інфраструктури.

5. В умовах воєнного стану спостерігаються негативні тенденції щодо поширення окремих кримінальних правопорушень, які завдають шкоди об'єктам критичної інфраструктури, зокрема відповідальність за які передбачена ст. 259, 360 КК України.

6. Проаналізовано судово-слідчу практику щодо особливостей кваліфікації кримінального правопорушення, передбаченого ч. 2 ст. 259 КК «Завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності». Зокрема, розглянуто питання кваліфікації за дії, якщо об'єктами завідомо неправдивого повідомлення стали критично важливі об'єкти інфраструктури або будівлі чи споруди, що забезпечують діяльність органів державної влади, або заклади охорони здоров'я, або заклади освіти; якщо воно спричинило тяжкі наслідки; якщо воно вчинене повторно.

Також наведено підстави для відмежування ст. 259 від ст. 296 КК України.

7. Проаналізовано судово-слідчу практику щодо особливостей кваліфікації кримінального правопорушення, передбаченого ч. 3 ст.

360 КК «Умисне пошкодження або руйнування телекомунікаційної мережі». Зокрема, відмічено, що пошкодження предметів, вказаних в диспозиції ст. 360, поєднане з незаконним викраденням їх складових, потребує додаткової кваліфікації за статтями, які передбачають кримінальну відповідальність за відповідні кримінальні правопорушення проти власності. Враховуючи, що до об'єктів критичної інфраструктури відносять об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам то умисне пошкодження або руйнування телекомунікаційної мережі чи технічних засобів телекомунікації, чи споруд електрозв'язку, що входять до складу телекомунікаційної мережі, що спричинило припинення надання телекомунікаційних послуг об'єктів оборони чи національної безпеки, вчинені з метою ослаблення держави, кваліфікуються за сукупністю кримінальних правопорушень, передбачених ч. 3 ст. 360 КК та ст. 113 КК.

Також наведено приклади кваліфікації за сукупністю кримінальних правопорушень за: ч. 3 ст. 360 КК та 411 КК України; ч. 3 ст. 360 КК та відповідними частинами та статтями корисливих кримінальних правопорушень проти власності (ст. 185–187 КК, ст. 189–191 КК).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. URL : http://eur-lex. europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.
2. International critical information infrastructure protection handbook. URL : https://subs.emis.de/LNI/Proceedings/Proceedings36/GI-Proceedings.36-7.pdf.
3. Law 8/2011 on the Measures for the Protection of Critical Infrastructure 2011. URL : http://www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf.
4. Law of 1 July 2011 on the security and protection of critical infrastructures. URL : https://www.nbb.be/en/articles/law-1-july-2011-security-and-protection-criticalinfrastructures-inofficial-translation.
5. Legislative Framework for CIP in Austria. URL: https://cipworkshop. events/wp-content/uploads/2017/10/S4-T2-Legislative_Framework_for_CIP_ in_Austria.pdf.
6. National Strategy for Critical Infrastructure Protection (CIP Strategy). URL : http://ccpic.mai.gov.ro/docs/Germania_cip_stategy.pdf.
7. National strategy for the protection of Switzerland against cyber risks. URL : https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncssmap/ National_strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf.
8. Regulation No. 317/2014 Coll. on the Determination of Important Information Systems and their Determination Criteria. URL : https://nukib.gov.cz/ download/publications_en/legislation/Decree_317_2014_EN_v1.0_final.pdf.
9. Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards. URL : https://www. gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf.
10. The Act for National Security and the Safeguarding and Defence of Classified Material (SEGNAC 1). URL : www.gns.gov.pt/media/1356/SEGNAC1.pdf.
11. The policy letter Protecting Critical Infrastructure. URL : https://english. nctv.nl/binaries/20150409-national-security-progress-letter-national-safety-2015_ tcm32-84272.pdf.
12. Вирок Бабушкінського районного суду м. Дніпропетровська від 19.06.2014 р. URL : https://reyestr.court.gov.ua/Review/39370342.
13. Вирок Володимир-Волинського міського суду Волинської області від 26.08.2021 р. URL : https://reyestr.court.gov.ua/Review/99182601.
14. Вирок Голосіївського районного суду м. Києва від 12.12.2023 р. URL : https://reyestr.court.gov.ua/Review/115695145.
15. Вирок Іллічівського міського суду Одеської області від 08.11.2023 р. URL : https://reyestr.court.gov.ua/Review/114757584.
16. Вирок Київського районного суду м. Одеси від 10.02.2023 р. URL : https://reyestr.court.gov.ua/Review/108903689.

17. Вирок Малиновського районного суду м. Одеси від 09.05.2023 р. URL : https://reyestr.court.gov.ua/Review/110874502.

18. Вирок Новоград-Волинського міськрайонного суду Житомирської області від 18.01.2024 р. URL : https://reyestr.court.gov.ua/Review/116384203.

19. Вирок Орджонікідзевського районного суду м. Запоріжжя від 01.07.2022 р. URL : https://reyestr.court.gov.ua/Review/105030909.

20. Вирок Суворовського районного суду м. Одеси від 22.05.2024 р. URL : https://reyestr.court.gov.ua/Review/119239171.

21. Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури (зі змін.): наказ адміністрації Держспецзв'язку від 06.10.2021 р. № 601. URL : https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601.

22. Про затвердження Порядку передачі комплектів обладнання підсистеми збору телеметрії інформаційно-комунікаційних систем (активні сенсори) системи виявлення вразливостей і реагування на кіберінциденти та кібератаки до об'єктів кіберзахисту 6 наказ адміністрації Держспецзв'язку від 24.06.2022 р. № 284. URL : https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-24-chervnya-2022-roku-284-pro-zatverdzhennya-poryadku-peredachi-komplektiv-obladnannya-pidsistemi-zbo.

23. Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами 6 наказ адміністрації Держспецзв'язку від 24.06.2022 № 284від 29.05.2023 р. № 463. URL : https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-29-05-2023-463-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-zabezpechennya-kiberzakhistu-avtomatizovanikh-sistem-upravlinnya-tekhnologichnimi-procesami.

24. Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: наказ адміністрації Держспецзв'язку від 03.07.2023 р. № 570. URL : https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-03-07-2023-570-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-reaguvannya-sub-yektami-zabezpechennya-kiberbezpeki-na-rizni-vidi-podii-u-kiberprostori.

25. Про затвердження Примірної публічної пропозиції про здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж і Методичних рекомендацій з розроблення публічної пропозиції про здійснення пошуку та виявления потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж: наказ адміністрації Держспецзв'язку від 14.07.2023 р. № 599. URL : https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-14-07-2023-599-pro-zatverdzhennya-primirnoyi-publichnoyi-propoziciyi-pro-zdiisnennya-poshuku-ta-viyavlennya-potenciinoyi-vrazlivosti.

26. Про затвердження Положення про систему захищеного доступу

державних органів до мережі Інтернет : наказ адміністрації Держспецзв'язку від 30.08.2023 р. № 771. URL : https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-pro-zatverdzhennya-polozhennya-pro-sistemu-zakhishenogo-dostupu-derzhavnikh-organiv-do-merezhi-internet-vid-30-serpnya-2023-roku-771.

27. Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту систем електронного документообігу: наказ адміністрації Держспецзв'язку від 30.08.2023 р. № 773. URL : https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-pidvishennya-rivnya-kiberzakhistu-sistem-elektronnogo-dokumentoobigu-vid-30-serpn.

28. Про затвердження форм подання відомостей до державного реєстру об'єктів критичної інформаційної інфраструктури: наказ адміністрації Держспецзв'язку від 02.09.2023 р. № 793. URL : https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-pro-zatverdzhennya-form-podannya-vidomostei-do-derzhavnogo-reyestru-ob-yektiv-kritichnoyi-informaciinoyi-infrastrukturi-vid-02-veres.

29. Про затвердження форми Плану захисту об'єкта критичної інфраструктури за проєктною загрозою національного рівня «кібератака/кіберінцидент : наказ адміністрації Держспецзв'язку від 04.10.2023 р. № 877. URL : https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-pro-zatverdzhennya-formi-planu-zakhistu-ob-yekta-kritichnoyi-infrastrukturi-za-proyektnoyu-zagrozoyu-nacionalnogo-rivnya-kiberataka.

30. Про затвердження Рекомендацій з розроблення плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «кібератака/кіберінцидент : наказ адміністрації Держспецзв'язку від 01.12.2023 р. № 1011. URL : https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-01-grudnya-2023-roku-1011-pro-zatverdzhennya-richnogo-planu-zdiisnennya-zakhodiv-derzhavnogo-naglyadu-kontrolyu-u-sferi-doderzha.

31. Документи міжнародних організацій та країн-партнерів у сфері кіберзахисту. *Державна служба спеціального зв'язку та захисту інформації України*. URL : https://cip.gov.ua/ua/news/perelik-dokumentiv-mizhnarodnikh-organizacii-ta-krayin-partneriv-u-sferi-kiberzakhistu.

32. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: Постанова Кабінету Міністрів України від 23.12.2020 р. № 1295. URL : https://zakon.rada.gov.ua/laws/show/1295-2020-п#Text.

33. Деякі питання об'єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 р. № 943. URL : https://zakon.rada.gov.ua/laws/show/943-2020-п#n82.

34. Деякі питання об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 р. № 1109. URL : https://zakon.rada.gov.ua/laws/show/1109-2020-п#n42.

35. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Постанова Кабінету Міністрів України від

04.04.2023 р. № 299. URL : https://zakon.rada.gov.ua/laws/show/299-2023-п#Text.

36. Основи законодавства України про охорону здоров'я: Закон України від 19.11.1992 р. в редакції від 19.04.2024 р. URL : https://zakon.rada.gov.ua/laws/show/2801-12#Text.

37. Про внесення змін до статті 259 Кримінального кодексу України щодо посилення відповідальності за завідомо неправдиве повідомлення про загрозу безпеці громадян: Закон України. URL : https://zakon.rada.gov.ua/laws/show/1292-20#n5.

38. Про електронні комунікації: Закон України від 16.12.2020 р. URL : https://zakon.rada.gov.ua/laws/show/1089-20#n2246.

39. Про освіту: Закон України від 05.09.2017 р. URL : https://zakon.rada.gov.ua/laws/show/2145-19#Text.

40. Про телекомунікації: Закон України від 18.11.2003 р. (втратив чинність). URL : https://zakon.rada.gov.ua/laws/show/1280-15#Text.

41. Калініченко Ю. В. Кримінальна відповідальність за завідомо неправдиве повідомлення про вчинення злочину: монографія. Харків : Право, 2018. 256 с.

42. Карчевський М. Протидія злочинності в Україні: інфорграфіка (2013 – 2024): інтерактивний довідник. URL : https://karchevskiy.com/i-dovidnyk/

43. Кириченко О. В. Кримінально-правові та кримінологічні аспекти протидії завідомо неправдивим повідомленням про загрозу громадській безпеці: дис. … канд. юрид. наук: спец. 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право». Харків, 2005. 234 с.

44. Кримінальний кодекс України. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

45. Мельник М. І., Хавронюк М. І. Науково-практичний коментар Кримінального кодексу України (10-е вид., перероб. та доп.). К. : В. Дако, 2018. 1360 с.

46. Об'єкти критичної інфраструктури та об'єкти критичної інформаційної інфраструктури в європейських країнах. Інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром на запит Апарату Верховної Ради України. URL : https://infocenter.rada.gov.ua/uploads/documents/29297.pdf.

47. Про судову практику в справах про знищення та пошкодження державного чи колективного майна шляхом підпалу або внаслідок порушення встановлених законодавством вимог пожежної безпеки: Постанова Пленуму Верховного Суду України від 02.07.1976 р. № 4. URL : https://zakon.rada.gov.ua/laws/show/v0004700-76#Text.

48. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. URL : https://zakon.rada.gov.ua/laws/show/2939-17#Text.

49. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. URL : https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

50. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної

інфраструктури: Постанова Кабінету Міністрів України від 19.06.2019 № 518. URL : https://zakon.rada.gov.ua/laws/show/518-2019-п#Text.

51. Про затвердження Положення про організаційно-технічну модель кіберзахисту: Постанова Кабінету Міністрів України від 29.12.2021 № 1426. URL : https://zakon.rada.gov.ua/laws/show/1426-2021-п#Text.

52. Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних: наказ від 02.12.2014 № 660. URL : https://zakon.rada.gov.ua/laws/show/z0090-15#n14.

53. Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних: Постанова Кабінету Міністрів України від 16.05.2023 № 497. URL : https://zakon.rada.gov.ua/laws/show/497-2023-п#Text.

54. Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті: наказ від 15.01.2016 № 20. URL : https://zakon.rada.gov.ua/laws/show/z0196-16#n13.

55. Про затвердження форм подання відомостей до державного реєстру об’єктів критичної інформаційної інфраструктури: наказ від 02.09.2023 № 793. URL : https://zakon.rada.gov.ua/rada/show/v0793519-23#Text.

56. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL : https://zakon.rada.gov.ua/laws/show/1882-20#Text.

57. Про оборону України: Закон України від 06.12.1991 № 1932-XII. URL : https://zakon.rada.gov.ua/laws/show/1932-12?find=1&text=критич#w1_1.

58. Про правовий режим воєнного стану: Закон України від 12.05.2015 № 389-VIII. URL : https://zakon.rada.gov.ua/laws/show/389-19#Text.

59. Про правовий режим надзвичайного стану: Закон України від 16.03.2000 № 1550-III. URL : https://zakon.rada.gov.ua/laws/show/1550-14?find=1&text=критич#w1_1.

60. Про функціонування єдиної транспортної системи України в особливий період: Закон України від 20.10.1998 № 194-XIV. URL : https://zakon.rada.gov.ua/laws/show/194-14?find=1&text=критич#Text.

61. Роз’яснення щодо заповнення форм надання відомостей до державного реєстру об’єктів критичної інформаційної інфраструктури. URL : https://cip.gov.ua›api›attachment›download.

62. Що таке об’єкти критичної інфраструктури. *SmartTender*. URL : https://smarttender.biz/terminy/view/ob-yekti-kritichnoyi-infrastrukturi/

63. Юріков О. О. Кримінальна відповідальність за умисне пошкодження або руйнування телекомунікаційної мережі: дис. на … д-ра філос. за спец. 081 – Право. Київ, 2021. 311 с.

ДОДАТКИ

ЗАКОН УКРАЇНИ

Про критичну інфраструктуру

(Відомості Верховної Ради (ВВР), 2023, № 5, ст. 13)

{Із змінами, внесеними згідно із Законами
№ 1909-IX від 18.11.2021
№ 2684-IX від 18.10.2022}

Цей Закон визначає правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури і є складовою законодавства у сфері національної безпеки.

Розділ I
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення основних термінів

1. У цьому Законі наведені нижче терміни вживаються в такому значенні:

1) безпека критичної інфраструктури – стан захищеності критичної інфраструктури, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість критичної інфраструктури;

2) життєво важливі функції та/або послуги – функції та/або послуги, реалізація яких забезпечується органами державної влади, органами місцевого самоврядування, установами, суб'єктами господарювання та організаціями будь-якої форми власності, збої, переривання та порушення надання яких призводять до швидких негативних наслідків для національної безпеки;

3) захист критичної інфраструктури - всі види діяльності, що виконуються перед або під час створення, функціонування, відновлення і реорганізації об'єкта критичної інфраструктури, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об'єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації;

4) ідентифікація об'єкта критичної інфраструктури – процедура віднесення об'єкта інфраструктури до об'єктів критичної інфраструктури;

5) інцидент безпеки критичної інфраструктури (далі – інцидент) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, зокрема внаслідок дії людського фактора) та/або таких, що мають ознаки несанкціонованого втручання в функціонування об'єкта критичної інфраструктури, які становлять загрозу його безпеці, системі управління технологічними процесами об'єкта критичної інфраструктури, створюють ймовірність порушення штатного режиму функціонування такого об'єкта (у тому числі зриву та/або блокування роботи, та/або несанкціонованого управління його ресурсами), ставлять під загрозу його захищеність;

6) категоризація об'єктів інфраструктури – віднесення об'єктів інфраструктури до категорій критичності об'єктів інфраструктури;

7) категорія критичності (критерії) об'єкта критичної інфраструктури – ступінь

(відносний рівень) важливості об'єкта критичної інфраструктури, класифікована (категоризована) залежно від його впливу на виконання життєво важливих функцій та/або надання життєво важливих послуг;

8) кризова ситуація – порушення або загроза порушення штатного режиму функціонування критичної інфраструктури чи окремого її об'єкта, реагування на яке потребує залучення додаткових сил і ресурсів;

9) критична інфраструктура – сукупність об'єктів критичної інфраструктури;

10) критична технологічна інформація – дані, що обробляються (приймаються, передаються, зберігаються) в системах управління технологічними процесами об'єктів критичної інфраструктури;

11) національна система захисту критичної інфраструктури – сукупність органів управління, сил та засобів центральних і місцевих органів виконавчої влади (військово-цивільних адміністрацій – у разі утворення), органів місцевого самоврядування, операторів критичної інфраструктури, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури;

12) несанкціоноване втручання – незаконні дії, що створили загрозу безпечному функціонуванню об'єкта критичної інфраструктури та призвели до одного або декількох з таких наслідків: порушили його безперервність і стійкість; створили реальні чи потенційні загрози для населення, суспільства, соціально-економічного стану, національної безпеки і оборони України;

13) об'єкти критичної інфраструктури – об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам;

14) оператор критичної інфраструктури – юридична особа будь-якої форми власності та/або фізична особа – підприємець, що на правах власності, оренди або на інших законних підставах здійснює управління об'єктом критичної інфраструктури та відповідає за його поточне функціонування;

15) охорона об'єктів критичної інфраструктури – комплекс режимних, інженерних, інженерно-технічних та інших заходів (крім заходів із захисту інформації та кіберзахисту об'єктів критичної інформаційної інфраструктури), які організовуються і проводяться суб'єктами національної системи захисту критичної інфраструктури з метою запобігання та/або недопущення чи припинення протиправних дій (актів несанкціонованого втручання) на об'єктах критичної інфраструктури;

16) паспорт безпеки – документ встановленої форми, який містить відомості про об'єкт критичної інфраструктури, а також комплекс заходів, що вживаються для захисту цього об'єкта від визначених для нього видів загроз (відомості, що містяться у паспорті безпеки, є інформацією з обмеженим доступом);

17) проектна загроза об'єкту критичної інфраструктури – документ встановленої форми, який визначає властивості, характеристики реальних і потенційних загроз об'єкту критичної інфраструктури, на зниження ймовірності реалізації яких має бути спрямовано функціонування системи захисту критичної інфраструктури;

18) реєстр об'єктів критичної інфраструктури – автоматизована система, що містить перелік найбільш важливої для життєдіяльності суспільства та держави критичної інфраструктури, щодо якої встановлюються особливі вимоги із забезпечення її безпеки та стійкості і здійснюється моніторинг їх дотримання;

19) режим функціонування критичної інфраструктури – визначені оператором умови та вимоги до функціонування критичної інфраструктури залежно від стану і динаміки розвитку ситуації (штатний режим функціонування; режим функціонування у кризовій ситуації; режим відновлення);

20) рівень критичності об'єкта критичної інфраструктури – відносна міра важливості об'єкта, якою враховується його вплив на можливість виконання життєво важливих

функцій та надання життєво важливих послуг;

21) сектор критичної інфраструктури – сукупність об'єктів критичної інфраструктури, які належать до одного сектору (галузі) економіки та/або мають спільну функціональну спрямованість;

22) секторальний орган у сфері захисту критичної інфраструктури – державний орган, визначений законодавством відповідальним за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури;

23) стійкість критичної інфраструктури – стан критичної інфраструктури, за якого забезпечується її спроможність функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після впливу загроз будь-якого виду;

24) функціональний орган у сфері захисту критичної інфраструктури – державний орган, визначений відповідальним за функціонування окремих державних систем захисту та реагування.

Стаття 2. Законодавство про критичну інфраструктуру та її захист

1. Законодавство про критичну інфраструктуру та її захист складають Конституція України, цей Закон, інші закони України, міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України, інші нормативно-правові акти, прийняті на виконання цього Закону.

Стаття 3. Сфера застосування цього Закону

1. Цей Закон регулює відносини у сфері функціонування та захисту критичної інфраструктури в цілому та її об'єктів у мирний час.

2. Особливості захисту та правового режиму об'єктів критичної інфраструктури в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, особливого періоду регулюються законами України «Про правовий режим воєнного стану», «Про правовий режим надзвичайного стану», «Про функціонування єдиної транспортної системи України в особливий період» та «Про оборону України».

3. Окремим законом регулюються відносини щодо забезпечення кіберзахисту та кібербезпеки об'єктів критичної інфраструктури.

Розділ II
ОСНОВНІ ЗАСАДИ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стаття 4. Засади державної політики у сфері захисту критичної інфраструктури

1. Захист критичної інфраструктури є складовою частиною забезпечення національної безпеки України.

2. Державна політика у сфері захисту критичної інфраструктури ґрунтується на засадах:

1) визнання необхідності забезпечення безпеки та стійкості критичної інфраструктури;

2) визначення законодавчих вимог до принципів, пріоритетів, стратегічних завдань, підходів щодо захисту критичної інфраструктури;

3) визначення суб'єктів національної системи захисту критичної інфраструктури, їх повноважень та засад відповідальності, порядку взаємодії;

4) створення умов та впровадження заходів, спрямованих на ефективне зниження і контроль за ризиками безпеки, на зниження ризику реалізації можливих загроз, ліквідацію та/або мінімізацію наслідків реалізованих загроз, кризових ситуацій та інших їх видів;

5) створення системи раннього виявлення загроз критичній інфраструктурі;

6) запровадження державно-приватного партнерства, взаємодії суб'єктів господарювання та населення з питань забезпечення захисту та стійкості критичної інфраструктури;

7) забезпечення міжнародного співробітництва у сфері захисту критичної

інфраструктури;

8) створення умов швидкого відновлення надання життєво важливих функцій та послуг у разі реалізації загроз і порушення функціонування критичної інфраструктури.

3. Державна політика у сфері захисту критичної інфраструктури спрямовується на формування комплексу організаційних, нормативно-правових, інженерно-технічних, ресурсних, інформаційно-аналітичних та методологічних заходів, спрямованих на забезпечення безпеки критичної інфраструктури.

Стаття 5. Мета та завдання державної політики у сфері захисту критичної інфраструктури:

1. Метою державної політики у сфері захисту критичної інфраструктури є забезпечення безпеки об'єктів критичної інфраструктури, запобігання проявам несанкціонованого втручання в їх функціонування, прогнозування та запобігання кризовим ситуаціям на об'єктах критичної інфраструктури.

2. До завдань формування і реалізації державної політики у сфері захисту критичної інфраструктури належать:

1) запобігання проявам несанкціонованого втручання в її функціонування, прогнозування та запобігання кризовим ситуаціям на об'єктах критичної інфраструктури;

2) попередження кризових ситуацій, що порушують безпеку критичної інфраструктури;

3) створення, впровадження, розвиток та забезпечення функціонування національної системи захисту критичної інфраструктури, у тому числі шляхом визначення уповноваженого органу у сфері захисту критичної інфраструктури України, а також визначення повноважень у сфері захисту критичної інфраструктури інших суб'єктів національної системи захисту критичної інфраструктури;

{Пункт 3 частини другої статті 5 із змінами, внесеними згідно із Законом № 2684-IX від 18.10.2022}

4) розроблення нормативно-правової та нормативно-технічної бази з питань забезпечення безпеки об'єктів критичної інфраструктури;

5) розроблення та реалізація державних цільових програм із захисту критичної інфраструктури;

6) розроблення комплексу заходів з контролю за ризиками безпеки, виявлення, запобігання та ліквідації наслідків інцидентів безпеки на об'єктах критичної інфраструктури;

7) встановлення обов'язкових вимог із забезпечення безпеки об'єктів критичної інфраструктури, їх захищеності на всіх етапах життєвого циклу, у тому числі під час створення, прийняття в експлуатацію, модернізації;

8) аналіз викликів та загроз, що впливають на стійкість критичної інфраструктури, оцінка стану її захищеності;

9) розроблення методології аналізу результативності державної політики у сфері захисту критичної інфраструктури;

10) підготовка, перепідготовка, підвищення кваліфікації, тренування працівників національної системи захисту критичної інфраструктури;

11) забезпечення взаємодії національної системи захисту критичної інфраструктури з відповідними міжнародними системами, насамперед європейськими та євроатлантичними.

Стаття 6. Основні принципи функціонування національної системи захисту критичної інфраструктури

1. До основних принципів функціонування національної системи захисту критичної інфраструктури належать:

1) єдність методологічних засад;

2) координованість;

3) державно-приватне партнерство;

4) безпека, захист та охорона інформації з обмеженим доступом;

5) міжнародне співробітництво.

Стаття 7. Рівні управління національною системою захисту критичної інфраструктури:

1. Національна система захисту критичної інфраструктури має такі рівні управління:

1) загальнодержавний рівень, управління на якому здійснюється Кабінетом Міністрів України, уповноваженим органом у сфері захисту критичної інфраструктури України, органами державної влади відповідно до розподілу повноважень згідно з цим Законом, іншими центральними органами виконавчої влади та державними органами, Національним банком України;

2) регіональний та галузевий рівні, управління на яких здійснюється центральними та місцевими органами виконавчої влади, визначеними в установленому законом порядку відповідальними за забезпечення формування та реалізацію державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури та відповідальними за функціонування окремих державних систем захисту та реагування;

3) місцевий рівень, управління на якому здійснюється місцевими органами виконавчої влади (військово-цивільними адміністраціями – у разі створення), органами місцевого самоврядування в межах повноважень, покладених на них цим Законом;

4) об'єктовий рівень, управління на якому здійснюється оператором критичної інфраструктури на підставі нормативно-правових та регуляторних актів у сфері захисту критичної інфраструктури.

Розділ ІІІ
КРИТИЧНА ІНФРАСТРУКТУРА УКРАЇНИ

Стаття 8. Віднесення об'єктів до критичної інфраструктури

1. Віднесення об'єктів до критичної інфраструктури здійснюється в порядку, встановленому Кабінетом Міністрів України.

Віднесення банків, інших об'єктів, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, платіжних організацій, учасників платіжних систем, операторів послуг платіжної інфраструктури здійснюється в порядку, встановленому Національним банком України.

Віднесення об'єктів до критичної інфраструктури, що здійснюють діяльність на ринках послуг, державне регулювання та нагляд за діяльністю яких здійснюють державні органи, здійснюється в порядку, встановленому такими державними органами.

2. Віднесення об'єктів до критичної інфраструктури здійснюється за сукупністю критеріїв, що визначають їх соціальну, політичну, економічну, екологічну значущість для забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку, зокрема для реалізації життєво важливих функцій та надання життєво важливих послуг, свідчать про існування загроз для них, можливість виникнення кризових ситуацій через несанкціоноване втручання в їх функціонування, припинення функціонування, людський фактор чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму.

3. До таких критеріїв належать:

1) виконання функцій із забезпечення життєво важливих національних інтересів;

2) існування викликів і загроз, що можуть виникати щодо об'єктів критичної інфраструктури;

3) ймовірність завдання значної шкоди нормальним умовам життєдіяльності населення;

4) уразливість таких об'єктів, тяжкість можливих негативних наслідків, внаслідок чого буде заподіяна значна шкода здоров'ю населення (визначається кількістю постраждалих, загиблих та осіб, які отримали значні травми, а також чисельністю евакуйованого населення); соціальній сфері (руйнація систем соціального захисту населення і надання соціальних послуг, втрата спроможності держави задовольнити критичні потреби суспільства); державному суверенітету (зниження обороноздатності, дискредитація іміджу країни,

дестабілізація системи державного управління та унеможливлення виконання державою своїх функцій); економіці (вплив на внутрішній валовий продукт, розмір економічних втрат, як прямих, так і непрямих); природним ресурсам загальнодержавного та місцевого значення;

5) масштабність негативних наслідків для держави, які впливають на діяльність стратегічно важливих об'єктів для кількох секторів життєзабезпечення чи призводять до втрати унікальних національно значущих активів, систем і ресурсів, матимуть тривалі наслідки для держави і позначаться на діяльності ряду інших секторів;

6) тривалість ліквідації таких наслідків та дія подальшого негативного впливу на інші сектори держави;

7) вплив на функціонування суміжних секторів критичної інфраструктури.

4. Об'єкти критичної інфраструктури, що не можуть належати:

– фізичним і юридичним особам – громадянам та/або резидентам держави, визнаної Верховною Радою України державою-агресором, або кінцевими бенефіціарними власниками яких є громадяни держави, визнаної Україною державою-агресором або державою-окупантом;

– юридичним особам, зареєстрованим згідно із законодавством держав, включених FATF до списку держав, що не співпрацюють у сфері протидії відмиванню доходів, одержаних злочинним шляхом, а також юридичним особам, 50 і більше відсотків статутного капіталу яких належать прямо або опосередковано таким особам, протягом року підлягають відчуженню.

Стаття 9. Сектори критичної інфраструктури

1. Для організації ефективного забезпечення безпеки і стійкості критичної інфраструктури з урахуванням специфіки забезпечення окремих життєво важливих функцій та/або послуг визначаються сектори критичної інфраструктури.

2. Для секторів критичної інфраструктури визначаються особливості реалізації державної політики у сфері захисту критичної інфраструктури. Формування та реалізацію державної політики у відповідних секторах здійснюють секторальні органи у сфері захисту критичної інфраструктури.

Секторальні органи у сфері захисту критичної інфраструктури складають та ведуть секторальні переліки об'єктів критичної інфраструктури.

3. Перелік секторів критичної інфраструктури та суб'єктів, відповідальних за формування та реалізацію державної політики у відповідних секторах національної системи захисту критичної інфраструктури (далі – Перелік), визначається Кабінетом Міністрів України. У разі необхідності внесення змін до Переліку Кабінет Міністрів України переглядає та змінює його виходячи з критеріїв критичності, визначених цим Законом.

4. До життєво важливих функцій та/або послуг, порушення яких призводить до негативних наслідків для національної безпеки України, належать, зокрема:

1) урядування та надання найважливіших публічних (адміністративних) послуг;
2) енергозабезпечення (у тому числі постачання теплової енергії);
3) водопостачання та водовідведення;
4) продовольче забезпечення;
5) охорона здоров'я;
6) фармацевтична промисловість;
7) виготовлення вакцин, стале функціонування біолабораторій;
8) інформаційні послуги;
9) електронні комунікації;
10) фінансові послуги;
11) транспортне забезпечення;
12) оборона, державна безпека;
13) правопорядок, здійснення правосуддя, тримання під вартою;

14) цивільний захист населення та територій, служби порятунку;

15) космічна діяльність, космічні технології та послуги;

16) хімічна промисловість;

17) дослідницька діяльність.

Стаття 10. Категоризація об’єктів критичної інфраструктури

1. Для визначення рівня вимог щодо забезпечення захисту об’єктів критичної інфраструктури відповідно до рівня їх важливості для забезпечення окремих життєво важливих функцій у межах секторів критичної інфраструктури здійснюється категоризація об’єктів критичної інфраструктури відповідно до категорій критичності, визначених цим Законом.

2. Установлюються такі категорії критичності об’єктів критичної інфраструктури:

1) І категорія критичності – особливо важливі об’єкти, які мають загальнодержавне значення, значний вплив на інші об’єкти критичної інфраструктури та порушення функціонування яких призведе до виникнення кризової ситуації державного значення;

2) ІІ категорія критичності – життєво важливі об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації регіонального значення;

3) ІІІ категорія критичності – важливі об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації місцевого значення;

4) IV категорія критичності – необхідні об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації локального значення.

3. Категоризація об’єктів критичної інфраструктури здійснюється секторальними органами у сфері захисту критичної інфраструктури відповідно до секторальної специфіки та вимог секторального законодавства.

4. Секторальні органи разом з операторами критичної інфраструктури здійснюють категоризацію об’єктів критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури відповідно до Методики категоризації об’єктів критичної інфраструктури, що затверджується Кабінетом Міністрів України, а в банківській та фінансовій системах – Національним банком України, у сферах, державне регулювання та нагляд за діяльністю яких здійснюють державні органи, – такими державними органами.

Стаття 11. Реєстр об’єктів критичної інфраструктури

1. Для цілей узгодження дій суб’єктів національної системи захисту критичної інфраструктури формується Реєстр об’єктів критичної інфраструктури (далі – Реєстр).

2. Збирання, узагальнення, попередній аналіз даних щодо об’єктів критичної інфраструктури та пропозиції щодо включення таких об’єктів до Реєстру в межах визначених секторів здійснюються секторальними органами у сфері захисту критичної інфраструктури.

3. Реєстр формується та ведеться уповноваженим органом у сфері захисту критичної інфраструктури України на основі пропозицій суб’єктів національної системи захисту критичної інфраструктури.

4. Після включення об’єкта до Реєстру секторальні органи у сфері захисту критичної інфраструктури повідомляють про це оператора об’єкта критичної інфраструктури для забезпечення паспортизації та захисту об’єкта критичної інфраструктури відповідно до вимог цього Закону.

5. Порядок ведення Реєстру, включення об’єктів до Реєстру, доступу та надання інформації з нього визначається Кабінетом Міністрів України.

6. Інформація про об’єкти критичної інфраструктури, що міститься в Реєстрі, є відкритою, загальнодоступною та безоплатною, крім інформації з обмеженим доступом. Розпорядник забезпечує цілодобовий доступ до відкритої інформації Реєстру на своєму офіційному веб-сайті.

7. Для посадових осіб суб’єктів національної системи захисту критичної інфраструктури, визначених статтею 14 цього Закону, інформація з Реєстру у зв’язку із здійсненням ними повноважень, передбачених законом, надається за суб’єктом права чи за об’єктом критичної інфраструктури в електронній формі шляхом безпосереднього

доступу до Реєстру, за умови ідентифікації відповідної посадової особи у порядку, встановленому Законом України »Про електронні довірчі послуги».

Стаття 12. Паспортизація об'єктів критичної інфраструктури:

1. З метою проведення аналізу можливих основних загроз та потенційних негативних наслідків для об'єктів критичної інфраструктури, запобігання та попередження виникнення таких загроз для критичної інфраструктури оператори об'єктів критичної інфраструктури готують і подають на погодження до відповідних секторальних органів у сфері захисту критичної інфраструктури, відповідного функціонального органу паспорт безпеки на кожний об'єкт критичної інфраструктури.

2. Паспорт безпеки на об'єкт критичної інфраструктури містить інформацію про ідентифікацію об'єкта та заходи щодо його захисту і безпеки, а також визначає перелік посад та відповідальних осіб, до завдань яких належать зв'язок та обмін інформацією з суб'єктами національної системи захисту критичної інфраструктури.

3. Паспорт безпеки розробляється (переглядається) з урахуванням визначених проектних загроз. Погодження паспорта безпеки на об'єкт критичної інфраструктури здійснюється безоплатно для усіх операторів об'єктів критичної інфраструктури незалежно від форми власності.

4. Вимоги до порядку розроблення та погодження паспорта безпеки на об'єкт критичної інфраструктури, його наповнення, зміст, порядок і строки подання встановлюються Кабінетом Міністрів України.

5. Національний банк України визначає з урахуванням вимог цього Закону порядок розроблення паспорта безпеки на об'єкти критичної інфраструктури, зміст і строки подання його банками, іншими особами, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, платіжними організаціями, учасниками платіжних систем, операторами послуг платіжної інфраструктури.

6. Оператор критичної інфраструктури несе відповідальність за достовірність даних, наведених у паспорті безпеки, своєчасність внесення до нього змін.

7. Відомості, що містяться у паспорті безпеки, є інформацією з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Розділ IV
НАЦІОНАЛЬНА СИСТЕМА ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стаття 13. Формування та реалізація державної політики у сфері захисту критичної інфраструктури

1. Кабінет Міністрів України забезпечує проведення державної політики у сфері захисту критичної інфраструктури України, організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи захисту критичної інфраструктури, визначає уповноважений орган з питань захисту критичної інфраструктури України.

2. Формування та реалізацію державної політики в окремих секторах критичної інфраструктури здійснюють секторальні та функціональні органи у сфері захисту критичної інфраструктури відповідно до визначених законом повноважень.

3. Формування та реалізацію державної політики у сфері захисту критичної інфраструктури, координацію діяльності суб'єктів національної системи захисту критичної інфраструктури забезпечує уповноважений орган у сфері захисту критичної інфраструктури України.

{Частина третя статті 13 в редакції Закону № 2684-IX від 18.10.2022}

4. Для забезпечення обміну інформацією та взаємодії суб'єктів національної системи захисту критичної інфраструктури Кабінет Міністрів України затверджує Регламент обміну інформацією.

5. Обмін інформацією в рамках функціонування національної системи захисту

критичної інфраструктури здійснюється відповідно до вимог законодавства у сфері захисту інформації.

Стаття 14. Суб'єкти національної системи захисту критичної інфраструктури

1. Суб'єктами національної системи захисту критичної інфраструктури є:

1) Кабінет Міністрів України;

2) Апарат Ради національної безпеки і оборони України;

3) Центральна виборча комісія;

4) Національний банк України;

5) Національна комісія з цінних паперів та фондового ринку, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг;

6) Адміністрація Державної служби спеціального зв'язку та захисту інформації України;

7) Фонд державного майна України, інші центральні органи виконавчої влади із спеціальним статусом;

8) уповноважений орган у сфері захисту критичної інфраструктури України;

9) центральний орган виконавчої влади, який забезпечує формування та реалізує державну політику у сфері цивільного захисту;

10) секторальні та функціональні органи, інші міністерства та центральні органи виконавчої влади;

11) Служба безпеки України;

12) правоохоронні та розвідувальні органи, суб'єкти оперативно-розшукової та контррозвідувальної діяльності;

13) Збройні Сили України, інші військові формування, утворені відповідно до законів України;

14) місцеві органи виконавчої влади (військово-цивільні адміністрації – у разі утворення);

15) органи місцевого самоврядування;

16) оператори критичної інфраструктури;

17) підприємства, установи та організації незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки та стійкості критичної інфраструктури.

Стаття 15. Режими функціонування національної системи захисту критичної інфраструктури:

1. Забезпечення захисту та стійкості критичної інфраструктури здійснюється в таких режимах її функціонування:

1) штатний режим – суб'єктами національної системи захисту критичної інфраструктури стосовно оцінки можливих загроз та інформування щодо них. Функціонування інфраструктури здійснюється відповідно до проектного цільового призначення;

2) режим готовності та запобігання реалізації загроз – секторальними та функціональними органами у сфері захисту критичної інфраструктури: проводиться перевірка та переведення системи захисту до готовності забезпечити захист та реагування на випадок реалізації загрози. Функціонування інфраструктури здійснюється відповідно до проектного цільового призначення;

3) режим реагування на виникнення кризової ситуації – суб'єктами національної системи захисту критичної інфраструктури із застосуванням заходів реагування на кризову ситуацію. Функціонування інфраструктури відбувається в режимі кризової ситуації, вводяться обмеження на режими роботи об'єктів інфраструктури, економічні умови господарювання, доступ до об'єктів;

4) режим відновлення штатного функціонування – суб'єктами національної системи захисту критичної інфраструктури: застосовуються заходи щодо повернення параметрів функціонування критичної інфраструктури до штатного режиму. Функціонування інфраструктури здійснюється з обмеженнями відповідно до визначених термінів ліквідації наслідків кризи.

2. Суб'єктами національної системи захисту критичної інфраструктури розробляється план взаємодії з іншими суб'єктами національної системи захисту, який погоджується

з уповноваженим органом у сфері захисту критичної інфраструктури України та затверджується Кабінетом Міністрів України і переглядається раз на три роки. У плані взаємодії можуть бути визначені особливості взаємодії для режимів функціонування національної системи захисту критичної інфраструктури.

3. Рішення про оголошення режимів функціонування критичної інфраструктури приймається секторальними органами у сфері захисту критичної інфраструктури, відповідальними за сектор критичної інфраструктури.

Стаття 16. Уповноважений орган у сфері захисту критичної інфраструктури України:

1. Уповноважений орган у сфері захисту критичної інфраструктури України забезпечує формування та реалізує державну політику у сфері захисту критичної інфраструктури, здійснює функціональне управління національною системою захисту критичної інфраструктури, забезпечує координацію діяльності міністерств та операторів критичної інфраструктури з питань забезпечення стійкості та захисту об'єктів критичної інфраструктури.

Діяльність уповноваженого органу у сфері захисту критичної інфраструктури України спрямовує, координує та контролює Кабінет Міністрів України.

{Абзац другий частини першої статті 16 в редакції Закону № 2684-IX від 18.10.2022}

2. Уповноважений орган у сфері захисту критичної інфраструктури України:

1) координує діяльність міністерств, інших центральних та місцевих органів виконавчої влади (військово-цивільних адміністрацій – у разі утворення) у сфері захисту критичної інфраструктури;

2) узагальнює пропозиції суб'єктів національної системи захисту критичної інфраструктури, формує та веде Реєстр;

3) взаємодіє з секторальними, функціональними органами у сфері захисту критичної інфраструктури та операторами критичної інфраструктури з питань забезпечення захисту об'єктів, включених до Реєстру;

4) організовує здійснення оцінки захищеності об'єктів критичної інфраструктури, внесених до Реєстру, аналізує та оцінює загальний стан їх захищеності;

5) проводить оцінку загроз критичній інфраструктурі на національному рівні та оцінку загроз національній безпеці внаслідок реалізації загроз критичній інфраструктурі із залученням секторальних та функціональних органів у сфері захисту критичної інфраструктури;

6) готує щорічну оцінку ризиків і загроз критичній інфраструктурі національного рівня;

7) погоджує проектні ризики та загрози критичній інфраструктурі секторального рівня;

8) готує рекомендації щодо визначення вимог до забезпечення захисту та стійкості секторів критичної інфраструктури відповідно до категорій об'єктів критичної інфраструктури;

9) надає пропозиції Кабінету Міністрів України щодо:

– Національного плану захисту та забезпечення стійкості критичної інфраструктури;

– порядку розроблення, форми та змісту паспорта безпеки об'єкта критичної інфраструктури;

– порядку розроблення, форми та змісту планів заходів щодо захисту критичної інфраструктури, які приймаються на національному рівні;

10) розробляє та затверджує Проектні загрози критичній інфраструктурі національного рівня, що становлять інформацію з обмеженим доступом;

11) готує висновки та рекомендації власнику/оператору критичної інфраструктури щодо зміни права власності, цільового призначення чи режиму функціонування об'єкта критичної інфраструктури;

12) забезпечує функціонування системи обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури;

13) створює бази даних щодо загроз і вразливостей критичній інфраструктурі;

14) забезпечує координацію секторальних органів, підготовку пропозицій до проектів стратегічних документів щодо забезпечення безпеки та стійкості, здійснення захисту критичної інфраструктури – Стратегії національної безпеки України, Стратегії кібербезпеки України та Стратегії громадської безпеки та цивільного захисту України;

15) бере участь у розробленні нової галузі знань, програм навчання, підвищення кваліфікації, робочих і навчальних програм з питань забезпечення стійкості та захисту критичної інфраструктури;

16) здійснює міжнародне співробітництво, забезпечує дотримання і виконання зобов'язань, взятих відповідно до міжнародних договорів України з питань захисту критичної інфраструктури, налагоджує і підтримує зв'язки з міжнародними організаціями, іноземними державами, їх правоохоронними органами і спеціальними службами;

17) здійснює інші повноваження, передбачені цим Законом.

3. Положення про уповноважений орган у сфері захисту критичної інфраструктури затверджується Кабінетом Міністрів України.

{Частина третя статті 16 в редакції Закону № 2684-IX від 18.10.2022}

Стаття 17. Функціональні органи у сфері захисту критичної інфраструктури

1. Органи державної влади, визначені відповідальними за функціонування окремих державних систем захисту та реагування:

1) беруть участь у встановленому законодавством порядку в реагуванні на кризові ситуації, пов'язані із забезпеченням безпеки та стійкості критичної інфраструктури;

2) готують пропозиції щодо включення об'єктів інфраструктури до Реєстру;

3) формують перелік об'єктів критичної інфраструктури, що належать до сфери їх управління;

4) надають власникам та операторам інфраструктури консультації щодо ризиків і загроз критичній інфраструктурі та заходів щодо їх нейтралізації;

5) здійснюють іншу діяльність для забезпечення стійкості та захисту критичної інфраструктури в межах повноважень, що регулюють діяльність суб'єктів захисту критичної інфраструктури, зокрема:

– організовують проведення оцінки загроз та ризиків критичній інфраструктурі у відповідних сферах;

– беруть участь у проведенні оцінки загроз та ризиків критичній інфраструктурі на загальнодержавному рівні;

– формують пропозиції щодо національних та секторальних проектних ризиків і загроз;

– забезпечують організацію взаємодії та обміну інформацією з іншими суб'єктами національної системи захисту критичної інфраструктури;

– здійснюють моніторинг рівня безпеки об'єктів критичної інфраструктури у відповідних сферах.

Стаття 18. Особливості діяльності окремих органів, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури

1. Діяльність Національного банку України, уповноваженого органу у сфері захисту критичної інфраструктури України, центрального органу виконавчої влади, який забезпечує формування та реалізує державну політику у сфері цивільного захисту, Служби безпеки України, Національної гвардії України, Національної поліції України, Збройних Сил України, Державної спеціальної служби транспорту та Державної служби спеціального зв'язку та захисту інформації України з питань формування та/або реалізації державної політики у сфері захисту критичної інфраструктури здійснюється в рамках, визначених цим Законом, та у порядку, встановленому законами України, що регламентують правові засади організації та діяльності зазначених у цій статті органів.

Стаття 19. Секторальні органи у сфері захисту критичної інфраструктури

1. Державні органи, визначені відповідальними за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури в окремому

секторі критичної інфраструктури, здійснюють такі завдання:

1) створюють у межах штатної чисельності у своєму складі структурні підрозділи з питань захисту критичної інфраструктури;

2) збирають, узагальнюють та здійснюють попередній аналіз даних щодо критичної інфраструктури та її функціонування;

3) спільно з операторами критичної інфраструктури здійснюють категоризацію об'єктів критичної інфраструктури своїх секторів критичної інфраструктури, формують секторальні переліки об'єктів критичної інфраструктури, подають інформацію до Реєстру;

4) розробляють та затверджують:

а) вимоги до захисту об'єктів критичної інфраструктури відповідно до їх категорій;

б) проектні загрози критичній інфраструктурі секторального рівня;

в) плани взаємодії функціональних органів у сфері захисту критичної інфраструктури у відповідних секторах для всіх режимів функціонування критичної інфраструктури; плани взаємодії та підтримання життєво важливих функцій на випадок порушення функціонування об'єктів критичної інфраструктури;

5) розробляють та впроваджують норми і регламенти захисту критичної інфраструктури у відповідних секторах критичної інфраструктури;

6) затверджують проектні загрози критичній інфраструктурі об'єктового рівня у відповідних секторах;

7) погоджують паспорти безпеки об'єктів критичної інфраструктури, надані операторами у відповідних секторах;

8) здійснюють:

а) перевірку та оцінку захищеності об'єктів критичної інфраструктури;

б) підготовку пропозицій до проектних ризиків та загроз критичній інфраструктурі національного рівня та щорічної оцінки ризиків і загроз критичній інфраструктурі національного рівня;

в) організацію системи підготовки персоналу, навчання та тренувань щодо забезпечення стійкості та захисту секторів критичної інфраструктури;

г) підготовку щорічного звіту щодо забезпечення захисту критичної інфраструктури у відповідному секторі;

д) участь у встановленому законодавством порядку в реагуванні на кризові ситуації, пов'язані з безпекою, захистом та стійкістю об'єктів критичної інфраструктури, а також у створенні умов для належного виконання правоохоронними, розвідувальними та контррозвідувальними органами своїх завдань щодо захисту критичної інфраструктури;

е) попередження про загрози операторів критичної інфраструктури та надають інформаційну, консультативну, експертну, методичну допомогу операторам критичної інфраструктури, користувачам їх послуг (населенню) задля попередження, реагування, мінімізації можливого впливу загроз;

9) надають операторам об'єктів критичної інфраструктури рекомендації з питань захисту критичної інфраструктури та обов'язкові до виконання вимоги щодо усунення причин і умов, які порушують стійкість критичної інфраструктури;

10) виконують:

а) збір, аналіз та узагальнення даних щодо об'єктів критичної інфраструктури та загроз їх функціонуванню;

б) заходи із функціонування відповідних систем обміну інформацією, моніторингу рівня безпеки об'єктів критичної інфраструктури;

11) організовують функціонування системи обміну інформацією та взаємодії у відповідних секторах критичної інфраструктури між суб'єктами національної системи захисту критичної інфраструктури;

12) готують пропозиції до стратегічних документів щодо забезпечення стійкості та захисту критичної інфраструктури.

2. Секторальні органи у сфері захисту критичної інфраструктури щороку відповідно до строків та форми звіту, затверджених Кабінетом Міністрів України, подають

інформацію уповноваженому органу у сфері захисту критичної інфраструктури України.

Стаття 20. Місцеві органи виконавчої влади та військово-цивільні адміністрації

1. Місцеві органи виконавчої влади (військово-цивільні адміністрації – у разі утворення) у сфері захисту критичної інфраструктури забезпечують:

1) розроблення та затвердження місцевих програм забезпечення безпеки та стійкості критичної інфраструктури, програм підвищення стійкості територіальних громад до кризових ситуацій, викликаних припиненням або погіршенням надання важливих для їх життєдіяльності послуг чи для здійснення життєво важливих функцій;

2) розроблення, затвердження та погодження із заінтересованими органами:

а) місцевих планів взаємодії залучених суб'єктів у кризовій ситуації з метою підтримання життєво важливих функцій та надання життєво важливих послуг, планів відновлення функціонування критичної інфраструктури;

б) програм навчання населення для забезпечення захисту в разі виникнення режиму реагування на виникнення кризової ситуації та режиму відновлення штатного функціонування.

Стаття 21. Завдання, права та обов'язки операторів критичної інфраструктури

1. Основними завданнями операторів критичної інфраструктури є:

1) забезпечення захисту об'єктів критичної інфраструктури, зокрема створення, налагодження та підтримання функціонування ефективної системи фізичної безпеки, безпеки операційних систем та кібербезпеки;

2) розроблення, оновлення та забезпечення виконання об'єктових планів заходів щодо забезпечення безпеки і стійкості критичної інфраструктури, правил управління ризиками безпеки, планів локалізації та ліквідації наслідків аварій, а також заходів кіберзахисту;

3) проведення оцінки ризиків на об'єктах критичної інфраструктури та обмін інформацією про ризики та загрози з іншими суб'єктами національної системи захисту критичної інфраструктури, а також створення умов для належного виконання правоохоронними, розвідувальними та контррозвідувальними органами своїх завдань щодо захисту критичної інфраструктури;

4) створення окремого структурного підрозділу або визначення відповідальної особи за організацію захисту критичної інфраструктури та забезпечення постійного зв'язку з відповідними суб'єктами національної системи захисту критичної інфраструктури;

5) оперативне реагування на протиправні дії, фізичні атаки, спрямовані на відключення або пошкодження роботи операційних систем чи систем забезпечення фізичної безпеки об'єкта критичної інфраструктури;

6) організація заходів з реагування на інциденти, кризові ситуації, а також ліквідації їх наслідків на об'єктах критичної інфраструктури у взаємодії з іншими суб'єктами національної системи захисту критичної інфраструктури;

7) забезпечення відновлення функціонування об'єктів критичної інфраструктури в разі виникнення аварій та інших небезпечних подій, вчинення протиправних дій;

8) участь у заходах із захисту повітряного простору над визначеними об'єктами критичної інфраструктури;

9) негайне інформування уповноваженого органу у сфері захисту критичної інфраструктури України, органів Національної поліції України, Служби безпеки України, підрозділів Національної гвардії України, інших державних органів про інциденти, пов'язані з порушеннями систем фізичної безпеки та кібербезпеки, а також інформування Служби безпеки України про загрози та ризики диверсій, терористичних актів, актів кібертероризму проти систем управління, операційних та інших систем об'єктів критичної інфраструктури, надзвичайних ситуацій або інших небезпечних подій на важливих державних об'єктах;

10) забезпечення постійного зв'язку з відповідальними за реагування на протиправні дії та з іншими компетентними організаціями та установами;

11) забезпечення постійної взаємодії з підприємствами, які забезпечують централізоване

водопостачання, централізоване водовідведення, постачання теплової енергії, енергопостачання, функціонування електронних комунікаційних мереж, транспортне обслуговування, медичну допомогу, безпеку та інші послуги, від яких залежить процес реагування на кризові ситуації та відновлення функціонування об'єктів критичної інфраструктури;

12) створення і використання необхідних резервів фінансових та матеріальних ресурсів для реагування на кризові ситуації та ліквідації їх наслідків;

13) проведення навчань та тренінгів, підготовка та перевірка персоналу, який відповідає за охорону, безпеку та захист об'єктів критичної інфраструктури;

14) захист інформації про системи управління, зв'язку, фізичну безпеку та кібербезпеку, забезпечення відповідно до встановлених законодавством вимог конфіденційності інформації під час оброблення даних про об'єкти критичної інфраструктури;

15) забезпечення захисту персоналу об'єктів критичної інфраструктури, організація та здійснення евакуаційних заходів у разі виникнення надзвичайних ситуацій.

2. Оператори критичної інфраструктури забезпечують розроблення та затвердження у встановленому законодавством порядку:

1) вимог щодо організації захисту об'єктів критичної інфраструктури;

2) посадових інструкцій осіб, відповідальних за організацію та забезпечення захисту об'єктів критичної інфраструктури;

3) проведення навчань та тренінгів, підготовку та перевірку персоналу, який відповідає за охорону, безпеку та захист об'єктів критичної інфраструктури;

4) паспортів безпеки об'єктів критичної інфраструктури.

3. Оператори критичної інфраструктури мають право:

1) отримувати в установленому порядку від уповноважених органів державної влади інформацію про забезпечення безпеки об'єктів критичної інфраструктури;

2) самостійно розробляти заходи щодо забезпечення безпеки об'єктів критичної інфраструктури, що не суперечать вимогам цього Закону та прийнятих відповідно до нього нормативно-правових актів;

3) отримувати від уповноваженого органу у сфері захисту критичної інфраструктури України консультації щодо застосування законодавства у сфері захисту критичної інфраструктури та вжиття необхідних заходів для захисту критичної інфраструктури.

4. Оператори критичної інфраструктури зобов'язані:

1) забезпечити захист об'єктів критичної інфраструктури;

2) невідкладно поінформувати відповідальних суб'єктів національної системи захисту критичної інфраструктури (секторальні та функціональні органи) про інциденти, що сталися на об'єктах критичної інфраструктури, які належать їм на праві власності або на іншій законній підставі;

3) завчасно, але не менше ніж за 30 календарних днів до дати зміни стану об'єкта критичної інфраструктури або його частини, інформувати уповноважений орган у сфері захисту критичної інфраструктури України про наміри змінити цільове призначення, режим функціонування чи намір передати права на об'єкт критичної інфраструктури та виконувати надані їм висновки та рекомендації;

4) щороку надавати інформацію про виконання повноважень відповідно до цього Закону за формою, визначеною Кабінетом Міністрів України.

Розділ V
ОРГАНІЗАЦІЙНІ ЗАСАДИ НАЦІОНАЛЬНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стаття 22. Планування заходів щодо забезпечення стійкості та захисту об'єктів критичної інфраструктури

1. Для організації функціонування національної системи захисту критичної інфраструктури Кабінетом Міністрів України, центральними органами виконавчої влади,

місцевими органами виконавчої влади (військово-цивільними адміністраціями – у разі створення), органами місцевого самоврядування розробляються та затверджуються відповідні плани та програми реагування на кризові ситуації.

Кабінет Міністрів України встановлює вимоги щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності, крім банків, інших осіб, які здійснюють діяльність на ринках фінансових послуг, платіжних організацій, учасників платіжних систем, операторів послуг платіжної інфраструктури, державне регулювання, нагляд за діяльністю яких здійснює Національний банк України, та встановлює вимоги щодо управління ризиками безпеки.

2. На державному рівні розробляється Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури, який затверджується Кабінетом Міністрів України.

3. На секторальному (галузевому) та регіональному рівнях органи державної влади розробляють і затверджують галузеві, регіональні плани та програми з протидії загрозам критичній інфраструктурі, включаючи аварійні плани, плани реагування на кризові ситуації, плани взаємодії, плани відновлення об'єктів критичної інфраструктури, плани проведення навчань та тренувань.

4. Національна поліція України, Національна гвардія України, Служба безпеки України, Збройні Сили України, Державна служба України з питань надзвичайних ситуацій та інші складові сектору безпеки і оборони у межах компетенції здійснюють планування відповідних заходів із захисту критичної інфраструктури.

5. На місцевому рівні: місцеві органи виконавчої влади (військово-цивільні адміністрації – у разі утворення), органи місцевого самоврядування забезпечують розроблення, затвердження і виконання місцевих програм підвищення стійкості територіальних громад до кризових ситуацій, викликаних припиненням надання чи погіршенням якості важливих для їх життєдіяльності послуг або припиненням здійснення життєво важливих функцій. Такі програми включають заходи із забезпечення безпеки та стійкості критичної інфраструктури, взаємодії суб'єктів національної системи захисту критичної інфраструктури, а також відновлення функціонування об'єктів критичної інфраструктури.

6. На об'єктовому рівні: оператори критичної інфраструктури на кожному об'єкті критичної інфраструктури розробляють та забезпечують виконання об'єктового плану заходів щодо захисту і забезпечення стійкості критичної інфраструктури, який включає заходи з фізичного захисту, протидії загрозам, ефективного зниження та контролю за ризиками безпеки, забезпечення безпеки інформації та кібербезпеки на об'єктах критичної інфраструктури.

7. Плани та програми, затверджені відповідно до цієї статті, є обов'язковими до виконання всіма суб'єктами національної системи захисту критичної інфраструктури.

Стаття 23. Здійснення моніторингу рівня безпеки об'єктів критичної інфраструктури

1. Моніторинг рівня безпеки об'єктів критичної інфраструктури здійснюється шляхом проведення оцінки стану захищеності об'єктів критичної інфраструктури.

Оцінка стану захищеності об'єктів критичної інфраструктури проводиться секторальними та функціональними органами у сфері захисту критичної інфраструктури відповідно до їх повноважень, визначених законом.

2. Метою здійснення моніторингу є встановлення відповідності стану захищеності об'єкта критичної інфраструктури вимогам законодавства, достовірності наданої інформації визначеним суб'єктам національної системи захисту критичної інфраструктури, надання методичної допомоги операторам об'єктів критичної інфраструктури в удосконаленні системи захисту критичної інфраструктури.

3. За результатами проведення моніторингу рівня безпеки готуються пропозиції щодо удосконалення системи захисту об'єктів критичної інфраструктури, оцінки стану безпеки об'єктів критичної інфраструктури секторальними та функціональними органами у сфері захисту критичної інфраструктури. Пропозиції щодо удосконалення системи захисту об'єктів критичної інфраструктури, підготовлені за результатами моніторингу

оцінки стану захищеності, є інформацією з обмеженим доступом.

4. Порядок здійснення моніторингу оцінки стану безпеки об'єктів критичної інфраструктури та його періодичність затверджуються Кабінетом Міністрів України.

Стаття 24. Взаємодія національної системи захисту критичної інфраструктури з іншими системами захисту у сфері національної безпеки

1. Для забезпечення безпеки і стійкості критичної інфраструктури до загроз усіх видів, реалізації національних інтересів, функціонування суспільства та забезпечення соціально-економічного розвитку національна система захисту критичної інфраструктури взаємодіє з іншими системами захисту у сфері національної безпеки:

1) з єдиною державною системою запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків, з територіальною та функціональною підсистемами, структурними підрозділами суб'єктів боротьби з тероризмом;

2) з національною системою захисту інформаційних ресурсів в інформаційно-телекомунікаційних системах;

3) з національною системою кібербезпеки;

4) з правоохоронними органами у сфері протидії злочинності, а також з контррозвідувальними та розвідувальними органами у сфері забезпечення державної безпеки;

5) з об'єднаною цивільно-військовою системою організації повітряного руху України;

6) з єдиною державною системою цивільного захисту;

7) з державною системою фізичного захисту з питань охорони і оборони важливих державних об'єктів, захищеності та охорони ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання державної власності, запобігання диверсіям, крадіжкам або будь-якому іншому неправомірному вилученню радіоактивних матеріалів, протидії незаконному використанню безпілотних літальних апаратів;

8) із системою захисту персональних даних.

2. Взаємодія між державними системами захисту здійснюється у разі загрози виникнення або виникнення:

1) протиправних дій (у тому числі із застосуванням безпілотних літальних апаратів), захоплення об'єктів критичної інфраструктури або важливих державних об'єктів, що загрожують безпеці громадян і порушують функціонування систем життєзабезпечення;

2) диверсій, терористичних актів, викрадення, навмисного знищення, пошкодження майна та інших дій на об'єктах критичної інфраструктури, важливих державних об'єктах, внаслідок яких загинули люди або заподіяно значну матеріальну шкоду;

3) масштабних кібератак, актів кібертероризму проти систем управління, операційних та інших систем об'єктів критичної інфраструктури;

4) надзвичайних ситуацій або інших небезпечних подій на об'єктах критичної інфраструктури та важливих державних об'єктах;

5) аварій та технічних збоїв, кризових ситуацій на об'єктах критичної інфраструктури, що створюють загрозу життю та здоров'ю персоналу таких об'єктів та місцевого населення.

3. Організація взаємодії між суб'єктами національної системи захисту критичної інфраструктури здійснюється шляхом:

1) оперативного обміну інформацією щодо виконання завдань із захисту критичної інфраструктури;

2) проведення спільних оперативних нарад керівного складу уповноваженого органу у сфері захисту критичної інфраструктури України, центральних та територіальних органів Національної поліції України, Служби безпеки України, Національної гвардії України, Збройних Сил України, Державної служби України з питань надзвичайних ситуацій та інших заінтересованих державних органів;

3) здійснення спільних заходів із захисту критичної інфраструктури за планами, що розробляються на загальнодержавному, галузевому, регіональному місцевому та об'єктовому рівнях;

4) проведення спільних командно-штабних, тактико-спеціальних навчань, спільних тренувань та занять із захисту, охорони, оборони, припинення злочинних дій, інцидентів та кібератак проти об’єктів критичної інформаційної інфраструктури;

5) регулярного уточнення розрахунків сил та засобів, що залучаються до спільного виконання завдань із захисту об’єктів критичної інфраструктури та важливих державних об’єктів;

6) спільних заходів з припинення протиправних дій проти об’єктів критичної інфраструктури або важливих державних об’єктів, що загрожують безпеці громадян і порушують функціонування таких об’єктів;

7) участі у реагуванні та ліквідації наслідків інцидентів, кризових ситуацій на об’єктах критичної інфраструктури;

8) координації дій з підтримання або відновлення правопорядку в місцях розташування об’єктів критичної інфраструктури у разі виникнення кризових ситуацій;

9) здійснення інших заходів, передбачених законодавством.

Стаття 25. Державно-приватне партнерство у сфері захисту критичної інфраструктури

1. Державно-приватне партнерство у сфері захисту критичної інфраструктури здійснюється шляхом:

1) обміну інформацією між державними органами, місцевими органами виконавчої влади (військово-цивільними адміністраціями – у разі утворення), органами місцевого самоврядування, операторами критичної інфраструктури, громадськими об’єднаннями, організаціями роботодавців, а також громадянами щодо загроз критичній інфраструктурі та реагування на кризові ситуації;

2) визначення повноважень та відповідальності державних органів і операторів критичної інфраструктури у сфері забезпечення безпеки та стійкості критичної інфраструктури;

3) визначення порядку взаємодії між державними органами та операторами критичної інфраструктури у різних режимах функціонування об’єктів критичної інфраструктури;

4) створення системи підготовки кадрів для сфери захисту критичної інфраструктури;

5) підвищення комплексних знань, навичок і умінь персоналу та керівного складу операторів критичної інфраструктури, персоналу суб’єктів господарювання, які провадять діяльність, пов’язану із забезпеченням безпеки об’єктів критичної інфраструктури, з питань реагування на кризові ситуації на таких об’єктах;

6) залучення експертного потенціалу наукових установ, професійних та громадських об’єднань до підготовки галузевих проектів та нормативно-правових актів у сфері захисту критичної інфраструктури;

7) залучення до виконання завдань із забезпечення сталого функціонування об’єктів критичної інфраструктури суб’єктів господарювання, які провадять діяльність, пов’язану із забезпеченням безпеки об’єктів критичної інфраструктури, громадських об’єднань та професійних організацій;

8) надання державними органами консультативної та практичної допомоги операторам критичної інфраструктури з питань реагування на кризові ситуації на об’єктах критичної інфраструктури;

9) організації забезпечення захисту персоналу об’єктів критичної інфраструктури від можливих загроз;

10) забезпечення резервування основних ресурсів для функціонування критичної інфраструктури у різних режимах;

11) організації системи оповіщення населення та суб’єктів господарювання про інциденти та кризові ситуації на об’єктах критичної інфраструктури;

12) створення системи самооцінки віднесення об’єктів критичної інфраструктури за критеріями, визначеними цим Законом, створення інформаційних ресурсів для підвищення рівня знань із захисту об’єктів критичної інфраструктури;

13) створення механізмів для саморегулювання, обміну інформацією між операторами

об’єктів критичної інфраструктури у певному секторі;

14) створення та підтримки розвитку систем сертифікації та оцінки відповідності у секторах критичної інфраструктури.

2. Державно-приватне партнерство у сфері захисту критичної інфраструктури здійснюється з урахуванням установлених законодавством особливостей правового режиму щодо окремих об’єктів критичної інфраструктури та окремих видів діяльності.

3. З метою забезпечення ефективної взаємодії представників громадськості, органів виконавчої влади та реального сектору економіки у формуванні та реалізації єдиної державної політики у сферах забезпечення захисту національних інтересів України у кіберпросторі та захисту об’єктів критичної інфраструктури можуть створюватися консультативно-дорадчі органи, об’єднання та мережі у порядку, встановленому законодавством.

Стаття 26. Проведення незалежного аудиту діяльності національної системи захисту критичної інфраструктури

1. Незалежна зовнішня оцінка діяльності уповноваженого органу у сфері захисту критичної інфраструктури України здійснюється шляхом проведення щорічного зовнішнього аудиту його діяльності. Зовнішній аудит діяльності уповноваженого органу у сфері захисту критичної інфраструктури України проводиться Рахунковою палатою.

2. Незалежна зовнішня оцінка діяльності національної системи захисту критичної інфраструктури здійснюється один раз на три роки Рахунковою палатою у визначеному нею порядку на підставі міжнародних стандартів оцінки.

3. Форма та зміст звіту про зовнішній аудит діяльності уповноваженого органу у сфері захисту критичної інфраструктури України затверджуються Кабінетом Міністрів України з урахуванням вимог цього Закону.

4. Відшкодування витрат, пов’язаних із проведенням щорічного зовнішнього аудиту, здійснюється за рахунок Державного бюджету України.

Стаття 27. Парламентський контроль у сфері захисту критичної інфраструктури

1. Контроль за дотриманням законодавства при здійсненні заходів із забезпечення захисту критичної інфраструктури здійснюється Верховною Радою України в порядку, визначеному Конституцією України. Комітет Верховної Ради України, до предмета відання якого належать питання національної безпеки і оборони, та комітет Верховної Ради України, до предмета відання якого належать питання кібербезпеки об’єктів критичної інформаційної інфраструктури, на своїх засіданнях розглядають звіт уповноваженого органу у сфері захисту критичної інфраструктури України про результати незалежного аудиту діяльності щодо ефективності системи забезпечення захисту критичної інфраструктури.

2. За результатами розгляду звіту уповноваженого органу у сфері захисту критичної інфраструктури України комітет Верховної Ради України, до предмета відання якого належать питання національної безпеки і оборони, може порушити питання про розгляд цих питань Верховною Радою України.

Стаття 28. Громадський нагляд у сфері захисту критичної інфраструктури

1. Право громадського нагляду у сфері захисту критичної інфраструктури реалізується громадянами України через громадські об’єднання, членами яких вони є, через депутатів місцевих рад, особисто шляхом звернення до Уповноваженого Верховної Ради України з прав людини або до державних органів у порядку, встановленому Конституцією України, Законом України «Про громадські об’єднання» та іншими законами України, участі у діяльності громадських рад при органах, що формують та забезпечують реалізацію державної політики у сфері забезпечення захисту критичної інфраструктури, проведення незалежного аудиту їх діяльності, право доступу до публічної частини звіту щодо забезпечення захисту об’єктів критичної інфраструктури.

2. Доступ до інформації у сфері захисту критичної інфраструктури для реалізації громадського нагляду здійснюється у порядку, передбаченому Законом України «Про

доступ до публічної інформації», та може бути обмежений виключно Законом України «Про державну таємницю».

Стаття 29. Відповідальність за порушення законодавства у сфері захисту критичної інфраструктури

1. Особи, винні у порушенні законодавства у сфері захисту критичної інфраструктури, несуть відповідальність згідно із законом.

Стаття 30. Фінансування заходів у сфері захисту критичної інфраструктури

1. Джерелами фінансування робіт і заходів із забезпечення захисту критичної інфраструктури є кошти державного і місцевих бюджетів, власні кошти операторів критичної інфраструктури, кредити банків, кошти міжнародної технічної допомоги та інші джерела, не заборонені законодавством.

Стаття 31. Міжнародне співробітництво у сфері захисту критичної інфраструктури

1. Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері захисту критичної інфраструктури з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною злочинністю та тероризмом.

2. Україна відповідно до міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, може брати участь у спільних заходах із забезпечення захисту критичної інфраструктури, зокрема у проведенні спільних навчань суб'єктів сектору безпеки і оборони в рамках заходів колективної оборони з дотриманням вимог законі» та «Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України».

3. Відповідно до законодавства у сфері зовнішніх зносин суб'єкти національної системи захисту критичної інфраструктури у межах своїх повноважень здійснюють міжнародну співпрацю безпосередньо на двосторонній або багатосторонній основі.

Стаття 32. Страхування ризиків

1. Оператор критичної інфраструктури зобов'язаний забезпечити страхування ризику настання кризової ситуації.

2. Перелік об'єктів критичної інфраструктури, включених до Реєстру, страхових ризиків настання кризової ситуації на таких об'єктах, які підлягають страхуванню, а також мінімальний ліміт відповідальності (у разі страхування відповідальності перед третіми особами) затверджуються Кабінетом Міністрів України, а щодо об'єктів критичної інфраструктури у сфері фінансових послуг – погоджуються з Національним банком України.

Розділ VI
ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ

1. Цей Закон набирає чинності з дня, наступного за днем його опублікування, та вводиться в дію через шість місяців з дня набрання ним чинності, крім частини другої статті 32 (щодо страхування об'єктів критичної інфраструктури), яка набирає чинності через три роки з дня набрання чинності цим Законом.

2. Внести зміни до таких законодавчих актів України:

1) частину другу статті 17 Кодексу цивільного захисту України (Відомості Верховної Ради України, 2013 р., № 34-35, ст. 458) після пункту 53 доповнити п'ятьма новими пунктами такого змісту:

«54) бере участь в реалізації державної політики у сфері захисту критичної інфраструктури шляхом захисту населення і територій від надзвичайних ситуацій, запобігання їх виникненню, ліквідації наслідків надзвичайних ситуацій, гасіння пожеж, здійснення державного нагляду (контролю) за додержанням і виконанням вимог законодавства у сфері цивільного захисту, пожежної та техногенної безпеки;

55) реалізує заходи державної політики у сфері захисту критичної інфраструктури щодо впровадження інженерно-технічних заходів цивільного захисту на об'єктах

критичної інфраструктури;

56) бере участь у межах компетенції в оцінці захищеності об'єктів критичної інфраструктури;

57) здійснює заходи щодо постійного та обов'язкового на договірній основі аварійно-рятувального обслуговування суб'єктів господарювання та окремих територій, на яких існує небезпека виникнення надзвичайних ситуацій, віднесених до об'єктів критичної інфраструктури, аварійно-рятувальними службами, що пройшли атестацію в установленому порядку;

58) у взаємодії з Міністерством внутрішніх справ України, Службою безпеки України забезпечує організацію захисту від терористичних посягань об'єктів аварійно-рятувальних служб, які залучаються і виконують свої функції на об'єктах критичної інфраструктури в разі виникнення надзвичайних ситуацій».

У зв'язку з цим пункт 54 вважати пунктом 59;

2) абзац четвертий частини першої статті 5 Закону України «Про оперативно-розшукову діяльність» (Відомості Верховної Ради України, 1992 р., № 22, ст. 303 із наступними змінами) викласти в такій редакції:

«Служби безпеки України – оперативними підрозділами Центрального управління, регіональних органів та органів військової контррозвідки»;

3) пункт «б» частини першої статті 38 Закону України «Про місцеве самоврядування в Україні» (Відомості Верховної Ради України, 1997 р., № 24, ст. 170 із наступними змінами) доповнити підпунктом 2^{-1} такого змісту:

«2^{-1}) вжиття необхідних заходів щодо захисту критичної інфраструктури, відновлення функціонування важливих державних об'єктів національної економіки, об'єктів критичної інфраструктури та об'єктів, які забезпечують життєдіяльність населення, підвищення стійкості громад до кризових ситуацій, викликаних припиненням або погіршенням надання важливих для їх життєдіяльності послуг чи припиненням здійснення життєво важливих функцій, взаємодія між суб'єктами національної системи захисту критичної інфраструктури з урахуванням вимог Закону України «Про критичну інфраструктуру»;

4) статтю 25 Закону України «Про місцеві державні адміністрації» (Відомості Верховної Ради України, 1999 р., № 20-21, ст. 190 із наступними змінами) доповнити пунктом 24 такого змісту:

«24) забезпечує захист критичної інфраструктури, відновлення функціонування важливих державних об'єктів національної економіки, об'єктів критичної інфраструктури та об'єктів, які забезпечують життєдіяльність населення, підвищення стійкості громад до кризових ситуацій, викликаних припиненням або погіршенням надання важливих для їх життєдіяльності послуг або припиненням здійснення життєво важливих функцій, взаємодію між суб'єктами національної системи захисту критичної інфраструктури»;

5) у статті 7 Закону України «Про Національний банк України» (Відомості Верховної Ради України, 1999 р., № 29, ст. 238 із наступними змінами):

пункт 33 викласти в такій редакції:

«33) забезпечує формування та ведення реєстру об'єктів критичної інформаційної інфраструктури у банківській системі України, визначає критерії та порядок віднесення об'єктів у банківській системі України до об'єктів критичної інформаційної інфраструктури, забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки у банківській системі України»;

доповнити пунктом 33^{-1} такого змісту:

«33^{-1}) забезпечує формування та реалізацію державної політики у сфері захисту критичної інфраструктури щодо банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, платіжних організацій, учасників платіжних систем, операторів послуг платіжної інфраструктури відповідно до закону, що визначає правові та організаційні

засади функціонування і захисту критичної інфраструктури»;

6) у пункті 3 статті 16 Закону України «Про правовий режим надзвичайного стану» (Відомості Верховної Ради України, 2000 р., № 23, ст. 176; 2013 р., № 15, ст. 99; 2014 р., № 12, ст. 178) слова «об'єктів, що забезпечують життєдіяльність населення та народного господарства» замінити словами «важливих об'єктів національної економіки та об'єктів критичної інфраструктури»;

7) у Законі України »Про Збройні Сили України» (Відомості Верховної Ради України, 2000 р., № 48, ст. 410 із наступними змінами):

у статті 1:

– частину четверту після слів «до здійснення заходів правового режиму воєнного і надзвичайного стану» доповнити словами «безпеки та захисту критичної інфраструктури», а після слів «ліквідації надзвичайних ситуацій природного і техногенного характеру» – словами «кризових ситуацій»;

після частини четвертої доповнити новою частиною такого змісту:

– «Збройні Сили України у сфері захисту критичної інфраструктури забезпечують організацію захисту військових об'єктів критичної інфраструктури Збройних Сил України від терористичних загроз, підготовку до застосування військ (сил) Збройних Сил України у разі вчинення терористичного акту в повітряному просторі або територіальному морі України, проведення заходів з підвищення рівня захищеності, усунення ризиків і загроз вибухопожежобезпеки арсеналів, баз та складів Збройних Сил України, виконання завдань з протиповітряного прикриття важливих об'єктів держави (критичної інфраструктури), перелік яких визначається Кабінетом Міністрів України».

У зв'язку з цим частини п'яту – дев'яту вважати відповідно частинами шостою – десятою;

8) у Законі України «Про оборону України» (Відомості Верховної Ради України, 2000 р., № 49, ст. 420 із наступними змінами):

у статті 3:

– абзац десятий після слів «єдиної державної системи цивільного захисту» доповнити словами «об'єктів критичної інфраструктури»;

– абзац тринадцятий після слів «підготовку національної економіки» доповнити словами «об'єктів критичної інфраструктури»;

– в абзаці сьомому статті 9 слова «живучості об'єктів національної економіки та державного управління» замінити словами «живучості важливих об'єктів національної економіки, об'єктів критичної інфраструктури та державного управління»;

– в абзаці третьому частини першої статті 13 слова «інших об'єктів інфраструктури» замінити словами «інших об'єктів критичної інфраструктури»;

9) абзац перший частини першої статті 73 Закону України «Про банки і банківську діяльність» (Відомості Верховної Ради України, 2001 р., № 5-6, ст. 30 із наступними змінами) після слів «масового знищення» доповнити словами «законодавства з питань захисту критичної інфраструктури, кіберзахисту та інформаційної безпеки»;

{Підпункт 10пункту 2 розділу VI втратив чинність на підставі Закону № 1909-IX від 18.11.2021}

11) абзац четвертий частини четвертої статті 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» (Відомості Верховної Ради України, 2005 р., № 26, ст. 347; 2020 р., № 42, ст. 349) замінити двома новими абзацами такого змісту:

– «жоден з елементів системи не може бути розташований, а власник такої системи або його офіційний представник не може бути юридичною особою (його представником), зареєстрованою на територіях України, на яких органи державної влади України тимчасово не здійснюють своїх повноважень, на територіях держав, визнаних Верховною Радою України державами-агресорами, на територіях держав, щодо яких

застосовані санкції відповідно до Закону України »Про санкції», та на територіях держав, які входять до митних союзів з такими державами;

– власник системи або його представник, який надає послуги з використанням системи, елементи якої розміщуються поза межами України, має бути юридичною особою, зареєстрованою в Україні, або мати свого офіційного представника в Україні».

У зв'язку з цим абзац п'ятий вважати абзацом шостим;

12) у Законі України »Про інформацію» (Відомості Верховної Ради України, 2011 р., № 32, ст. 313 із наступними змінами):

статтю 10 після абзацу десятого доповнити новим абзацом такого змісту:

– «критична технологічна інформація».

У зв'язку з цим абзац одинадцятий вважати абзацом дванадцятим;

– доповнити статтею 19^{-1} такого змісту:

«**Стаття 19^{-1}**. Критична технологічна інформація

1. Критична технологічна інформація – дані, що обробляються (приймаються, передаються, зберігаються) в системах управління технологічними процесами об'єктів критичної інфраструктури.

2. Правовий режим критичної технологічної інформації визначається законами України та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

3. Критична технологічна інформація за режимом доступу належить до інформації з обмеженим доступом та підлягає захисту згідно із законом»;

13) частину другу статті 6 Закону України «Про охоронну діяльність» (Відомості Верховної Ради України, 2013 р., № 2, ст. 8) викласти в такій редакції:

«2. Перелік об'єктів критичної інфраструктури, охорона яких здійснюється державними органами, підприємствами та організаціями, затверджується Кабінетом Міністрів України»;

14) пункт 5 частини першої статті 20 Закону України «Про Кабінет Міністрів України» (Відомості Верховної Ради України, 2014 р., № 13, ст. 222; 2021 р., № 29, ст. 234) після абзацу сьомого доповнити трьома новими абзацами такого змісту:

– «забезпечує здійснення заходів із запобігання загрозам безпеці критичної інфраструктури та забезпечення безпеки критичної інфраструктури;

– забезпечує планування відновлення функціонування критичної інфраструктури у випадках надзвичайних ситуацій, яким не можна запобігти;

– забезпечує стійкість критичної інфраструктури до ідентифікованих загроз і небезпек».

У зв'язку з цим абзаци восьмий і дев'ятий вважати відповідно абзацами одинадцятим і дванадцятим;

15) частину першу статті 2 Закону України «Про Національну гвардію України» (Відомості Верховної Ради України, 2014 р., № 17, ст. 594 із наступними змінами) доповнити пунктом 5^{-1} такого змісту:

«5^{-1}) охорона об'єктів критичної інфраструктури, перелік яких визначається Кабінетом Міністрів України; участь у ліквідації наслідків кризових ситуацій на об'єктах критичної інфраструктури, що нею охороняються»;

16) у Законі України »Про Державну службу спеціального зв'язку та захисту інформації України» (Відомості Верховної Ради України, 2014 р., № 25, ст. 890 із наступними змінами):

у частині першій статті 3:

– абзац третій після слів «довірчих послуг» доповнити словами «захисту критичної інформаційної інфраструктури»;

– доповнити абзацами п'ятим – сьомим такого змісту:

– «реалізація державної політики щодо захисту критичної технологічної інформації, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснення державного контролю в цих сферах;

– визначення вимог до захисту критичної технологічної інформації, формування загальних вимог до кіберзахисту об’єктів критичної інфраструктури, ведення переліку об’єктів критичної інформаційної інфраструктури, здійснення заходів щодо його оновлення та актуалізації;

– виконання інших завдань, передбачених законодавством у сфері забезпечення кібербезпеки та кіберзахисту»;

пункт 24 частини першої статті 14 після слів «захисту інформації» доповнити словами «кіберзахисту об’єктів критичної інфраструктури»;

17) у Законі України »Про правовий режим воєнного стану» (Відомості Верховної Ради України, 2015 р., № 28, ст. 250; 2021 р., № 41, ст. 339):

частину першу, абзаци перший і другий частини сьомої, друге речення частини восьмої статті 4 після слів «громадської безпеки і порядку» доповнити словами «захисту критичної інфраструктури»;

у частині першій статті 8:

– у пункті 1 слова «об’єктів державного значення, об’єктів державного значення національної транспортної системи України» замінити словами «об’єктів критичної інфраструктури»;

– у пункті 2 слова «та сфері забезпечення життєдіяльності населення» і «та системи забезпечення життєдіяльності населення» замінити словами «та захисту критичної інфраструктури»;

– пункт 9 після слів «посягання на» доповнити словами «стійкість критичної інфраструктури»;

у статті 15:

– частину першу після слів «Про мобілізаційну підготовку та мобілізацію» доповнити словами «Про критичну інфраструктуру»;

– у пункті 25 частини другої слова «важливих об’єктів національної економіки» замінити словами «об’єктів критичної інфраструктури»;

– у пункті 7 частини третьої слова «важливих об’єктів національної економіки» замінити словами «об’єктів критичної інфраструктури»;

18) у частині першій статті 23 Закону України «Про Національну поліцію» (Відомості Верховної Ради України, 2015 р., № 40-41, ст. 379 із наступними змінами):

пункт 20 доповнити словами «а також об’єктів критичної інфраструктури, перелік яких визначається Кабінетом Міністрів України»;

– доповнити пунктом 24^{-1} такого змісту:

«24^{-1}) здійснює у визначеному законом порядку протидію злочинним посяганням на об’єкти критичної інфраструктури, які загрожують безпеці громадян і порушують функціонування систем життєзабезпечення; захист об’єктів критичної інфраструктури, інтересів суспільства і держави від злочинних посягань у кіберпросторі, здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів проти об’єктів критичної інфраструктури»;

19) у Законі України »Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради України, 2017 р., № 45, ст. 403; із змінами, внесеними Законом України від 30 червня 2021 року № 1591-IX):

у статті 1:

– пункт 16 частини першої виключити;

– частину другу доповнити реченням такого змісту: «Термін «об’єкт критичної інфраструктури» вживається в цьому Законі у значенні, визначеному Законом України «Про критичну інфраструктуру»;

– частини першу і другу статті 6 викласти в такій редакції:

«1. Віднесення об’єктів до об’єктів критичної інфраструктури та формування Реєстру об’єктів критичної інфраструктури здійснюються відповідно до Закону України

«Про критичну інфраструктуру».

2. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, у тому числі щодо застосування індикаторів кіберзагроз, та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Кабінетом Міністрів України, а в банківській системі України – Національним банком України»;

20) частину четверту статті 3 Закону України «Про національну безпеку України» (Відомості Верховної Ради України, 2018 р., № 31, ст. 241) викласти в такій редакції:

«4. Державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України та на інші її напрями».

3. До приведення у відповідність із цим Законом законодавчі та інші нормативно-правові акти застосовуються в частині, що не суперечить цьому Закону.

4. Перша щорічна незалежна зовнішня оцінка діяльності уповноваженого органу у сфері захисту критичної інфраструктури України має бути проведена після першого повного календарного року його діяльності починаючи відлік часу з календарного року, у якому такий орган приступив до здійснення своїх повноважень.

Перша незалежна зовнішня оцінка діяльності національної системи захисту критичної інфраструктури має бути проведена після спливу перших трьох календарних років діяльності уповноваженого органу у сфері захисту критичної інфраструктури України.

5. Кабінету Міністрів України:

1) у тримісячний строк з дня набрання чинності цим Законом:

– визначити уповноважений орган з питань захисту критичної інфраструктури України;

– забезпечити прийняття нормативно-правових актів, необхідних для реалізації цього Закону;

– привести свої нормативно-правові акти у відповідність із цим Законом;

– забезпечити приведення міністерствами, іншими центральними і місцевими органами виконавчої влади (військово-цивільними адміністраціями – в разі утворення) їх нормативно-правових актів у відповідність із цим Законом;

2) організувати та забезпечити виконання функцій уповноваженого органу з питань захисту критичної інфраструктури України в межах відповідних видатків на поточний рік державного органу, на який покладено такі повноваження;

3) під час підготовки проекту Державного бюджету України на 2022 рік та наступні роки врахувати видатки, необхідні для виконання повноважень (функцій) уповноваженого органу з питань захисту критичної інфраструктури України.

5^{-1}. Установити, що під час дії воєнного стану, а також протягом 12 місяців після його припинення чи скасування повноваження уповноваженого органу у сфері захисту критичної інфраструктури України, передбачені цим Законом, здійснюються Державною службою спеціального зв'язку та захисту інформації України.

{Розділ VI доповнено пунктом 5^{1} згідно із Законом № 2684-IX від 18.10.2022}

5^{-2}. Кабінету Міністрів України протягом 12 місяців після припинення чи скасування воєнного стану визначити уповноважений орган у сфері критичної інфраструктури України.

{Розділ VI доповнено пунктом 5^{2} згідно із Законом № 2684-IX від 18.10.2022}

6. Кабінету Міністрів України протягом трьох років з дня набрання чинності цим Законом забезпечити проведення та завершення перевірки структури власності об'єктів критичної інфраструктури з метою убезпечення належності таких об'єктів фізичним і юридичним особам – громадянам та/або резидентам держави, визнаної Верховною Радою України державою-агресором, або кінцевими бенефіціарними власниками яких є громадяни держави, визнаної Україною державою-агресором або державою-окупантом; юридичним особам, зареєстрованим згідно із законодавством держав, включених FATF до списку держав, що не співпрацюють у сфері протидії відмиванню доходів, одержаних злочинним

шляхом, а також юридичним особам, 50 і більше відсотків статутного капіталу яких належать прямо або опосередковано таким особам.

7. Кабінету Міністрів України до 1 січня 2024 року поінформувати Верховну Раду України про стан виконання цього Закону.

8. Рекомендувати Центральній виборчій комісії, Антимонопольному комітету України, Національному банку України, Національній комісії з цінних паперів та фондового ринку, Національній комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, Національній комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг, протягом трьох місяців з дня набрання чинності цим Законом:

– привести свої нормативно-правові акти у відповідність із цим Законом;

– забезпечити прийняття нормативно-правових актів, необхідних для реалізації цього Закону.

9. Центральному органу виконавчої влади у сфері освіти і науки спільно з уповноваженим органом у сфері захисту критичної інфраструктури України забезпечити проведення науково-дослідної роботи щодо доповнення Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, новою позицією у сфері забезпечення стійкості та захисту критичної інфраструктури та до 1 січня 2024 року поінформувати про результати Кабінет Міністрів України і подати проект відповідного рішення та пропозиції щодо програм навчання, підвищення кваліфікації, робочих і навчальних програм.

10. Уповноваженому органу у сфері захисту критичної інфраструктури України щороку починаючи з наступного дня за днем набрання чинності цим Законом забезпечити:

– проведення науково-дослідних робіт щодо впливу новітніх і проривних технологій на формування нових індикаторів потенційних ризиків та загроз об'єктам критичної інфраструктури;

– перегляд нормативно-правових актів у сфері захисту об'єктів критичної інфраструктури за результатами проведення науково-дослідних робіт;

– підготовку рекомендацій для операторів об'єктів критичної інфраструктури за результатами проведення науково-дослідних робіт;

– подання пропозицій щодо обсягів бюджетного фінансування для проведення уповноваженим органом у сфері захисту критичної інфраструктури України таких науково-дослідних робіт починаючи відлік часу з календарного року, у якому такий орган приступив до здійснення своїх повноважень;

– постійне інформування про результати Кабінету Міністрів України.

11. Уповноваженому органу у сфері захисту критичної інфраструктури України протягом року з дня початку ним діяльності підготувати зміни до Закону України «Про критичну інфраструктуру» в частині визначення форм та розмірів штрафних санкцій до операторів об'єктів критичної інфраструктури, до Кодексу України про адміністративні правопорушення, Кримінального кодексу України в частині визначення видів правопорушень та відповідальності за них.

Президент України **В. ЗЕЛЕНСЬКИЙ**

м. Київ
16 листопада 2021 року
№ 1882-IX

ЗАКОН УКРАЇНИ

Про основні засади забезпечення кібербезпеки України

(Відомості Верховної Ради (ВВР), 2017, № 45, ст.403)

{Із змінами, внесеними згідно із Законами
№ 2469-VIII від 21.06.2018, ВВР, 2018, № 31, ст.241
№ 720-IX від 17.06.2020, ВВР, 2020, № 47, ст.408
№ 912-IX від 17.09.2020
№ 1591-IX від 30.06.2021 – вводиться в дію з 01.08.2022
№ 1882-IX від 16.11.2021
№ 1907-IX від 18.11.2021
№ 1953-IX від 14.12.2021
№ 2130-IX від 15.03.2022
№ 2470-IX від 28.07.2022
№ 3549-IX від 16.01.2024}

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

1) індикатори кіберзагроз – показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;

2) інформація про інцидент кібербезпеки – відомості про обставини кіберінциденту, зокрема про те, які об'єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз;

3) інцидент кібербезпеки (далі – кіберінцидент) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;

4) кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання

несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;

5) кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

6) кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів;

7) кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;

8) кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

9) кіберзлочинність – сукупність кіберзлочинів;

10) кібероборона – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії;

11) кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних;

12) кіберрозвідка – діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням;

13) кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням;

14) кібершпигунство – шпигунство, що здійснюється у кіберпросторі або з його використанням;

15) критична інформаційна інфраструктура – сукупність об'єктів критичної інформаційної інфраструктури;

{Пункт 16 частини першої статті 1 виключено на підставі Закону № 1882-IX від 16.11.2021}

17) Національна телекомунікаційна мережа – сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв'язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, призначена для обігу (передавання, приймання, створення, оброблення, зберігання) та захисту національних інформаційних ресурсів, забезпечення захищених електронних комунікацій, надання спектра сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, та яка є мережею (системою) подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим споживачам;

18) національні електронні інформаційні ресурси (далі – національні інформаційні ресурси) – систематизовані електронні інформаційні ресурси, які містять інформацію

незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів;

18^{-1}) Національний центр резервування державних інформаційних ресурсів – організована сукупність об'єктів, створених з метою забезпечення надійності та безперебійності роботи державних інформаційних ресурсів, кіберзахисту, зберігання національних електронних інформаційних ресурсів, резервного копіювання інформації та відомостей національних електронних інформаційних ресурсів державних органів, військових формувань, утворених відповідно до законів, підприємств, установ та організацій;

{Частину першу статті 1 доповнено пунктом 18^{-1} згідно із Законом № 1907-IX від 18.11.2021}

19) об'єкт критичної інформаційної інфраструктури – комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури;

20) система управління технологічними процесами (далі – технологічна система) – автоматизована або автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання, інші технічні та технологічні засоби) незалежно від наявності доступу системи до мережі Інтернет та/або інших глобальних мереж передачі даних;

21) системи електронних комунікацій (далі – комунікаційні системи) – системи передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв'язку, електричні кабельні мережі в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв'язку, комп'ютери, інша комп'ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних;

22) система активної протидії агресії у кіберпросторі – сукупність організаційних, правових, наукових та технічних заходів, спрямованих на підвищення рівня кіберзахисту держави шляхом здійснення впливу на інформаційні (автоматизовані), електронно-комунікаційні, інформаційно-комунікаційні системи держави-агресора, джерела походження кіберзагроз та кібератак;

{Частину першу статті 1 доповнено пунктом 22 згідно із Законом № 2470-IX від 28.07.2022}

23) активна протидія агресії у кіберпросторі – дії, спрямовані на підвищення рівня кіберзахисту шляхом нейтралізації кібератак держави-агресора, його систем і мереж, а також джерел походження кіберзагроз та кібератак, які використовуються для завдання шкоди національній безпеці України.

{Частину першу статті 1 доповнено пунктом 23 згідно із Законом № 2470-IX від 28.07.2022}

Терміни «національна безпека», «національні інтереси», «загрози національній безпеці» вживаються в цьому Законі у значенні, визначеному Законом України «Про основи національної безпеки України». Термін «об'єкт критичної інфраструктури» вживається в цьому Законі у значенні, визначеному Законом України «Про критичну інфраструктуру».

{Частина друга статті 1 із змінами, внесеними згідно із Законом № 1882-IX від 16.11.2021}

Термін «платіжний ринок» вживається в цьому Законі у значенні, наведеному в Законі України «Про платіжні послуги».

{Статтю 1 доповнено частиною третьою згідно із Законом № 1591-IX від

30.06.2021 – вводиться в дію з 01.08.2022}

Стаття 2. Принципи застосування Закону

1. Цей Закон не поширюється на:

1) відносини та послуги, пов'язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах;

2) діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення;

3) соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсів;

4) комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем).

2. Застосування законодавства у сфері кібербезпеки та прийняття суб'єктами владних повноважень рішень на виконання норм цього Закону здійснюються з додержанням принципів:

1) мінімально необхідного регулювання, згідно з яким рішення (заходи) суб'єктів владних повноважень повинні бути необхідними і мінімально достатніми для досягнення мети і завдань, визначених цим Законом;

2) об'єктивності та правової визначеності, максимально можливого застосування національного та міжнародного права щодо повноважень і обов'язків державних органів, підприємств, установ, організацій, громадян у сфері кібербезпеки;

3) забезпечення захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, та/або послуг із захисту інформації, кіберзахисту, у тому числі прав щодо невтручання у приватне життя і захисту персональних даних;

4) прозорості, згідно з яким рішення (заходи) суб'єктів владних повноважень мають бути належним чином обґрунтовані та повідомлені суб'єктам, яких вони стосуються, до набрання ними чинності (їх застосування);

5) збалансованості вимог та відповідальності, згідно з яким має бути забезпечено баланс між встановленням відповідальності за невиконання вимог кібербезпеки та кіберзахисту, а також за запровадження надмірних вимог та обмежень;

6) недискримінації, згідно з яким рішення, дії та бездіяльність суб'єктів владних повноважень не можуть призводити до юридичного або фактичного обсягу прав та обов'язків особи, який є:

– відмінним від обсягу прав та обов'язків інших осіб у подібних ситуаціях, якщо тільки така відмінність не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу;

– таким, як і обсяг прав та обов'язків інших осіб у неподібних ситуаціях, якщо така однаковість не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу;

7) еквівалентності вимог до забезпечення кібербезпеки об'єктів критичної інфраструктури, згідно з яким застосування правових норм повинно бути якомога більш рівнозначним щодо кіберзахисту комунікаційних та технологічних систем об'єктів критичної інфраструктури, що належать до одного сектору економіки та/або які здійснюють аналогічні функції.

Зазначені принципи застосовуються без переваги будь-якого з них з урахуванням мети і завдань цього Закону.

Стаття 3. Правові основи забезпечення кібербезпеки України

1. Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних

ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

2. Якщо міжнародним договором України, згоду на обов'язковість якого надано Верховною Радою України, передбачено інші правила, ніж встановлені цим Законом, застосовуються положення міжнародного договору України.

Стаття 4. Об'єкти кібербезпеки та кіберзахисту

1. Об'єктами кібербезпеки є:

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

5) об'єкти критичної інфраструктури.

2. Об'єктами кіберзахисту є:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

2) об'єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

3. Порядок формування переліку об'єктів критичної інформаційної інфраструктури, перелік таких об'єктів та порядок їх внесення до державного реєстру об'єктів критичної інформаційної інфраструктури, а також порядок формування та забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури затверджуються Кабінетом Міністрів України.

Повноваження щодо формування та забезпечення функціонування реєстру об'єктів критичної інформаційної інфраструктури у банківській системі України та на ринках небанківських фінансових послуг, регулювання та нагляд за діяльністю на яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг покладаються на Національний банк України.

{Абзац другий частини третьої статті 4 зі змінами, внесеними згідно із Законом № 1953-IX від 14.12.2021}

Стаття 5. Суб'єкти забезпечення кібербезпеки

1. Координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України.

2. Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України.

3. Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській

системі України та на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг).

{Частина третя статті 5 із змінами, внесеними згідно із Законом № 1953-IX від 14.12.2021}

4. Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є:

1) міністерства та інші центральні органи виконавчої влади;

2) місцеві державні адміністрації;

3) органи місцевого самоврядування;

4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

5) Збройні Сили України, інші військові формування, утворені відповідно до закону;

6) Національний банк України;

7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;

8) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

5. Суб'єкти забезпечення кібербезпеки у межах своєї компетенції:

1) здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

2) здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

3) здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

4) розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

5) забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління;

6) здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору.

Стаття 6. Об'єкти критичної інфраструктури

2. Віднесення об'єктів до об'єктів критичної інфраструктури та формування Реєстру об'єктів критичної інфраструктури здійснюються відповідно до Закону України «Про критичну інфраструктуру».

{Частина перша статті 6 в редакції Закону № 1882-IX від 16.11.2021; /-зміни до пункту 1 частини першої статті 6, прийняті Законом № 1591-IX від 30.06.2021 – вводиться в дію з 01.08.2022, внести неможливо (відсутній пункт 1)-/}

2. Критерії та порядок віднесення об'єктів до об'єктів критичної інфраструктури, перелік таких об'єктів, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз, та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Кабінетом Міністрів України, а щодо банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг – Національним банком України.

{Частина друга статті 6 в редакції Законів № 1882-IX від 16.11.2021, № 1591-IX від 30.06.2021 – вводиться в дію з 01.08.2022}

3. Вимоги і порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури встановлюються відповідними нормативно-правовими актами з аудиту інформаційної безпеки, що затверджуються Кабінетом Міністрів України.

Розроблення нормативно-правових актів з незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури здійснюється на основі міжнародних стандартів, стандартів Європейського Союзу та НАТО з обов'язковим залученням представників основних суб'єктів національної системи кібербезпеки, наукових установ,

незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій.

4. Відповідальність за забезпечення кіберзахисту комунікаційних і технологічних систем об'єктів критичної інфраструктури, захисту технологічної інформації відповідно до вимог законодавства, за невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA про інциденти кібербезпеки, за організацію проведення незалежного аудиту інформаційної безпеки на таких об'єктах покладається на власників та/або керівників підприємств, установ та організацій, віднесених до об'єктів критичної інфраструктури.

5. Обмін інформацією про інциденти кібербезпеки, що містить персональні дані, здійснюється з дотриманням вимог Закону України »Про захист персональних даних».

Стаття 7. Принципи забезпечення кібербезпеки

1. Забезпечення кібербезпеки в Україні ґрунтується на принципах:

1) верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом;

2) забезпечення національних інтересів України;

3) відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі;

4) державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері;

5) пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;

6) пріоритетності запобіжних заходів;

7) невідворотності покарання за вчинення кіберзлочинів;

8) пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;

9) міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях;

10) забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки.

Стаття 8. Національна система кібербезпеки

1. Національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.

2. Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, які відповідно до Конституції і законів України виконують в установленому порядку такі основні завдання:

1) Державна служба спеціального зв'язку та захисту інформації України забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, активної протидії агресії у кіберпросторі, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує

діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; забезпечує функціонування Державного центру кіберзахисту та Центру активної протидії агресії у кіберпросторі, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA;

{Пункт 2 частини другої статті 8 із змінами, внесеними згідно із Законом № 2470-IX від 28.07.2022}

2) Національна поліція України забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від кримінально протиправних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі;

{Пункт 2 частини другої статті 8 із змінами, внесеними згідно із Законом № 720-IX від 17.06.2020}

3) Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки;

{Пункт 3 частини другої статті 8 із змінами, внесеними згідно із Законом № 720-IX від 17.06.2020}

4) Міністерство оборони України розробляє, затверджує план кіберзахисту у відповідній сфері управління та визначає особливості його реалізації щодо інформаційних, інформаційно-комунікаційних, електронних комунікаційних систем, власником (розпорядником) яких є Міністерство оборони України, Збройні Сили України та інші утворені відповідно до законів України військові формування, за умови, якщо такі системи не взаємодіють з будь-якими іншими системами та не використовуються для забезпечення надання електронних публічних послуг; здійснює військову співпрацю з НАТО; здійснює в межах своєї компетенції міжнародне співробітництво за воєнно-політичними, військово-технічними та іншими напрямами, а також з питань цивільно-військових відносин з відповідними органами іноземних держав та міжнародними організаціями у сфері кібероборони; визначає в межах своєї компетенції особливості вимог безпеки інформації до постачальників (їх субпідрядників) товарів, робіт та послуг оборонного призначення;

{Пункт 4 частини другої статті 8 в редакції Закону № 3549-IX від 16.01.2024}

5) розвідувальні органи України здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки;

6) Національний банк України визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки банками, іншими особами, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторами платіжних систем та/або учасниками платіжних систем, технологічними операторами платіжних послуг, здійснює контроль за їх виконанням; створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту для банків, інших осіб, що

здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг; забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури в банках, інших особах, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторах платіжних систем та/або учасниках платіжних систем, технологічних операторах платіжних послуг.

{Пункт 6 частини другої статті 8 в редакції Закону № 1591-IX від 30.06.2021 – вводиться в дію з 01.08.2022}

3. Функціонування національної системи кібербезпеки забезпечується шляхом:

1) вироблення і оперативної адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО;

2) створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО;

3) встановлення обов'язкових вимог інформаційної безпеки об'єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об'єкти критичної інформаційної інфраструктури;

4) формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту;

5) залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;

6) проведення навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі;

7) функціонування системи аудиту інформаційної безпеки, запровадження кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;

8) розвитку мережі команд реагування на комп'ютерні надзвичайні події;

9) розвитку та вдосконалення системи технічного і криптографічного захисту інформації;

10) забезпечення дотримання вимог законодавства щодо захисту державних інформаційних ресурсів та інформації;

11) створення та забезпечення функціонування Національної телекомунікаційної мережі;

12) обміну інформацією про інциденти кібербезпеки між суб'єктами забезпечення кібербезпеки у порядку, визначеному законодавством;

13) впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту;

14) підготовки фахівців освітньо-кваліфікаційних рівнів бакалавра і магістра за державним замовленням в обсязі, необхідному для задоволення потреб державного сектору економіки, а також за небюджетні кошти, у тому числі для підвищення кваліфікації та проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури, з урахуванням міжнародних стандартів;

15) впровадження організаційно-технічної моделі національної системи кібербезпеки як комплексу заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем;

16) встановлення вимог (правил, настанов) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами;

17) державно-приватної взаємодії у запобіганні кіберзагрозам об'єктам критичної інфраструктури, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період;

18) періодичного проведення огляду національної системи кібербезпеки, розроблення індикаторів стану кібербезпеки;

19) стратегічного планування та програмно-цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту;

20) розвитку міжнародного співробітництва у сфері кібербезпеки, підтримки міжнародних ініціатив у сфері кібербезпеки, що відповідають національним інтересам України, поглиблення співпраці України з Європейським Союзом та НАТО з метою посилення спроможності України у сфері кібербезпеки, участі у заходах із зміцнення довіри при використанні кіберпростору, що проводяться під егідою Організації з безпеки і співробітництва в Європі;

21) здійснення оперативно-розшукових, розвідувальних, контррозвідувальних та інших заходів, спрямованих на запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються з використанням кіберпростору, розслідування, переслідування, оперативного реагування та протидії кіберзлочинності, розвідувально-підривній, терористичній та іншій діяльності у кіберпросторі, що завдає шкоди інтересам України, використанню мережі Інтернет у воєнних цілях;

{Пункт 21 частини третьої статті 8 із змінами, внесеними згідно із Законом № 720-IX від 17.06.2020}

22) здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, сектору безпеки і оборони з використанням кіберпростору, створення і розвитку сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватися як засіб стримування воєнних конфліктів та загроз з використанням кіберпростору;

23) обмеження участі у заходах із забезпечення інформаційної безпеки та кібербезпеки будь-яких суб'єктів господарювання, які перебувають під контролем держави, визнаної Верховною Радою України державою-агресором, або держав та осіб, стосовно яких діють спеціальні економічні та інші обмежувальні заходи (санкції), прийняті на національному або міжнародному рівні внаслідок агресії щодо України, а також обмеження використання продукції, технологій та послуг таких суб'єктів для забезпечення технічного та криптографічного захисту державних інформаційних ресурсів, посилення державного контролю в цій сфері;

24) розвитку системи контррозвідувального забезпечення кібербезпеки, призначеної для запобігання, своєчасного виявлення та протидії зовнішнім і внутрішнім загрозам безпеці України з використанням кіберпростору; усунення умов, що їм сприяють, та причин їх виникнення;

25) проведення розвідувальних заходів із виявлення та протидії загрозам національній безпеці України у кіберпросторі, виявлення інших подій і обставин, що стосуються сфери кібербезпеки.

4. Порядок функціонування Національної телекомунікаційної мережі, критерії, правила та вимоги щодо надання послуг, їх тарифікації для користувачів бюджетної сфери, відшкодування витрат державного бюджету на утримання Національної телекомунікаційної мережі затверджуються Кабінетом Міністрів України.

5. Впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки здійснюється Державним центром кіберзахисту, який забезпечує створення та функціонування основних складових системи захищеного

доступу державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури, системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, системи взаємодії команд реагування на комп'ютерні надзвичайні події, а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань.

6. Органи державної влади, військові формування, утворені відповідно до законів України, державні підприємства, установи та організації з метою усунення можливих наслідків кіберінцидентів та кібератак створюють резервні копії національних електронних інформаційних ресурсів, що перебувають у їх володінні або розпорядженні та є критичними для їх сталого функціонування, та передають їх на зберігання до Національного центру резервування державних інформаційних ресурсів, крім тих, передача яких обмежена законодавством. Порядок передачі, збереження і доступу до зазначених копій визначається Кабінетом Міністрів України.

Національний центр резервування державних інформаційних ресурсів забезпечує:

1) безперервність роботи відповідного національного електронного інформаційного ресурсу, резервного копіювання інформації та відомостей національного електронного інформаційного ресурсу через єдині основний та резервний захищені центри обробки даних (дата-центри), призначені для обробки національних електронних інформаційних ресурсів, резервного копіювання національних електронних інформаційних ресурсів;

2) надійне функціонування серверного обладнання, системи зберігання даних, активного мережевого обладнання, архітектурно-технічних рішень щодо резервного копіювання й дублювання інформаційних систем, постійно працюючої інженерної інфраструктури;

3) здійснення обов'язкового контролю за статистичними даними роботи з фізичного захисту об'єктів, системи управління та моніторингу інформаційних систем, комплексу організаційних заходів;

4) розроблення, створення (побудову), модернізацію, розвиток, впровадження та супроводження програмного забезпечення інформаційної системи (платформи) для побудови та ведення реєстрів;

5) переміщення протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування резервних копій національних електронних інформаційних ресурсів до електронних комунікаційних мереж закордонних дипломатичних установ України в порядку, встановленому Кабінетом Міністрів України.

{Частину шосту статті 8 доповнено пунктом 5 згідно із Законом № 2130-IX від 15.03.2022}

{Статтю 8 доповнено частиною шостою згідно із Законом № 1907-IX від 18.11.2021}

Стаття 9. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA

1. Завданнями CERT-UA є:

1) накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

2) надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів;

3) організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;

4) підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;

5) взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;

6) взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти

безпеки FIRST із сплатою щорічних членських внесків;

7) взаємодія 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;

8) опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;

9) сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам.

2. Забезпечення функціонування CERT-UA здійснює Державна служба спеціального зв'язку та захисту інформації України у межах штатної чисельності та виділених обсягів фінансування.

Стаття 10. Державно-приватна взаємодія у сфері кібербезпеки

3. Державно-приватна взаємодія у сфері кібербезпеки здійснюється шляхом:

1) створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;

2) підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;

3) обміну інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об'єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів;

4) партнерства та координації команд реагування на комп'ютерні надзвичайні події;

5) залучення експертного потенціалу, наукових установ, професійних об'єднань та громадських організацій до підготовки ключових галузевих проектів та нормативних документів у сфері кібербезпеки;

6) надання консультативної та практичної допомоги з питань реагування на кібератаки;

7) формування ініціатив та створення авторитетних консультаційних пунктів для громадян, представників промисловості та бізнесу з метою забезпечення безпеки в мережі Інтернет;

8) запровадження механізму громадського контролю ефективності заходів із забезпечення кібербезпеки;

9) періодичного проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки;

10) створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки;

11) тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, IT-компаніями з метою виконання заходів кібероборони в кіберпросторі.

2. Державно-приватна взаємодія у сфері кібербезпеки застосовується з урахуванням встановлених законодавством особливостей правового режиму щодо окремих об'єктів та окремих видів діяльності.

Стаття 11. Сприяння суб'єктам забезпечення кібербезпеки України

Державні органи та органи місцевого самоврядування, їх посадові особи, підприємства, установи та організації незалежно від форми власності, особи, громадяни та об'єднання громадян зобов'язані сприяти суб'єктам забезпечення кібербезпеки, повідомляти відомі їм дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об'єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії

кіберзлочинам, кібератакам та мінімізації їх наслідків.

Стаття 12. Відповідальність за порушення законодавства у сфері кібербезпеки

Особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації, якщо кіберпростір є місцем та/або способом здійснення кримінального правопорушення, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним законодавством, несуть відповідальність згідно із законом.

{Стаття 12 із змінами, внесеними згідно із Законом № 720-IX від 17.06.2020}

Стаття 13. Фінансове забезпечення заходів кібербезпеки

Джерелами фінансування робіт і заходів із забезпечення кібербезпеки та кіберзахисту є кошти державного і місцевих бюджетів, власні кошти суб'єктів господарювання, кредити банків, кошти міжнародної технічної допомоги та інші джерела, не заборонені законодавством.

Стаття 14. Міжнародне співробітництво у сфері кібербезпеки

1. Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю.

2. Україна відповідно до міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, може брати участь у спільних заходах із забезпечення кібербезпеки, зокрема у проведенні спільних навчань суб'єктів сектору безпеки і оборони в рамках заходів колективної оборони з дотриманням вимог законів України «Про порядок направлення підрозділів Збройних Сил України до інших держав» та «Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України».

3. Відповідно до законодавства України у сфері зовнішніх зносин суб'єкти забезпечення кібербезпеки у межах своїх повноважень можуть здійснювати міжнародну співпрацю у сфері кібербезпеки безпосередньо на двосторонній або багатосторонній основі.

4. Інформацію з питань, пов'язаних із боротьбою з міжнародною кіберзлочинністю, Україна надає іноземній державі на підставі запиту, додержуючись вимог законодавства України та її міжнародно-правових зобов'язань. Така інформація може бути надана без попереднього запиту іноземної держави, якщо це не перешкоджає проведенню досудового розслідування чи судового розгляду справи і може сприяти компетентним органам іноземної держави у припиненні кібератаки, своєчасному виявленні і припиненні кримінального правопорушення з використанням кіберпростору.

Стаття 15. Контроль за законністю заходів із забезпечення кібербезпеки України

1. Контроль за дотриманням законодавства при здійсненні заходів із забезпечення кібербезпеки здійснюється Верховною Радою України в порядку, визначеному Конституцією України.

Парламентський контроль за дотриманням законодавства про захист персональних даних та доступ до публічної інформації у сфері кібербезпеки здійснюється Уповноваженим Верховної Ради України з прав людини.

2. Контроль за діяльністю із забезпечення кібербезпеки суб'єктів сектору безпеки і оборони, інших державних органів здійснюється Президентом України та Кабінетом Міністрів України в порядку, визначеному Конституцією і законами України.

3. Незалежний аудит діяльності основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, щодо ефективності системи забезпечення кібербезпеки держави проводиться щороку згідно з міжнародними стандартами аудиту.

Звіти про результати проведення незалежного аудиту діяльності основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, щодо ефективності системи забезпечення кібербезпеки держави за попередній рік подаються Президентові України, Верховній Раді України та Кабінету Міністрів України у

сорокап’ятиденний строк після закінчення календарного року.

Комітет Верховної Ради України, до предмета відання якого належать питання національної безпеки і оборони, та Комітет Верховної Ради України, до предмета відання якого належать питання інформатизації та зв’язку, на своїх засіданнях розглядають звіти основних суб’єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, про результати незалежного аудиту їхньої діяльності щодо ефективності системи забезпечення кібербезпеки держави.

Основні суб’єкти національної кібербезпеки, визначені частиною другою статті 8 цього Закону, подають один раз на рік звіти про стан виконання ними заходів з питань забезпечення кібербезпеки держави, віднесених до їх компетенції, які мають містити, зокрема, інформацію про результати проведення незалежного аудиту їхньої діяльності.

За результатами розгляду звітів основних суб’єктів національної кібербезпеки Комітет Верховної Ради України, до предмета відання якого належать питання інформатизації та зв’язку, може порушити питання про розгляд цих питань Верховною Радою України.

ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ

1. Цей Закон набирає чинності через шість місяців з дня його опублікування.

2. Внести зміни до таких законів України:

1) статтю 7 Закону України «Про Національний банк України» (Відомості Верховної Ради України, 1999 р., № 29, ст. 238 із наступними змінами) доповнити пунктами 32 і 33 такого змісту:

«32) визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб’єктів переказу коштів, здійснює контроль за їх виконанням; утворює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту у банківській системі України;

33) забезпечує формування та ведення переліку об’єктів критичної інфраструктури, а також реєстру об’єктів критичної інформаційної інфраструктури у банківській системі України, визначає критерії та порядок віднесення об’єктів у банківській системі України до об’єктів критичної інфраструктури та об’єктів критичної інформаційної інфраструктури, забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки у банківській системі України»;

2) у Законі України «Про оборону України» (Відомості Верховної Ради України, 2000 р., № 49, ст. 420; 2011 р., № 4, ст. 27; 2015 р., № 16, ст. 110; 2016 р., № 33, ст. 564):

а) статтю 3 після абзацу дев’ятнадцятого доповнити новим абзацом такого змісту:

«здійснення заходів з кібероборони (активного кіберзахисту) для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії».

У зв’язку з цим абзац двадцятий вважати абзацом двадцять першим;

б) друге речення частини другої статті 4 доповнити словами «у тому числі проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі»;

{Підпункт 3 пункту 2 розділу втратив чинність на підставі Закону № 912-IX від 17.09.2020}

{Підпункт 4 пункту 2 розділу втратив чинність на підставі Закону № 2469-VIII від 21.06.2018}

5) абзац шостий статті 3 Закону України «Про Службу зовнішньої розвідки України» (Відомості Верховної Ради України, 2006 р., № 8, ст. 94) після слів «національній безпеці України» доповнити словами «у тому числі у кіберпросторі»;

6) у Законі України «Про Державну службу спеціального зв’язку та захисту інформації України» (Відомості Верховної Ради України, 2014 р., № 25, ст. 890, № 29, ст. 946):

а) частину першу статті 2 та абзац другий частини першої статті 3 після слів «криптографічного та технічного захисту інформації» доповнити словом «кіберзахисту»;

б) у частині першій статті 14:

– пункт 39 після слів «забезпечення функціонування» доповнити словом «урядової»;

– доповнити пунктами 85-92 такого змісту:

«85) формування та реалізація державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, здійснення державного контролю у цих сферах;

86) координація діяльності суб'єктів забезпечення кібербезпеки щодо кіберзахисту;

87) забезпечення створення та функціонування Національної телекомунікаційної мережі;

88) впровадження організаційно-технічної моделі кіберзахисту, здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків;

89) інформування про кіберзагрози та відповідні методи захисту від них;

90) забезпечення впровадження системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлення вимог до аудиторів інформаційної безпеки, їх атестації (переатестації);

91) координація, організація та проведення аудиту захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість;

92) забезпечення функціонування Державного центру кіберзахисту».

3. Кабінету Міністрів України у тримісячний строк з дня набрання чинності цим Законом:

– забезпечити прийняття нормативно-правових актів, необхідних для реалізації цього Закону;

– привести свої нормативно-правові акти у відповідність із цим Законом;

– забезпечити перегляд і скасування міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів, що суперечать цьому Закону.

Президент України **П. ПОРОШЕНКО**

м. Київ
5 жовтня 2017 року
№ 2163-VIII

КАБІНЕТ МІНІСТРІВ УКРАЇНИ
ПОСТАНОВА

від 9 жовтня 2020 р. № 1109
Київ

Деякі питання об’єктів критичної інфраструктури

{Із змінами, внесеними згідно з Постановами КМ
№ 1414 від 29.12.2021
№ 991 від 02.09.2022
№ 1384 від 16.12.2022
№ 455 від 09.05.2023
№ 48 від 16.01.2024}

Відповідно до частини першої статті 8, частини третьої статті 9 та частини четвертої статті 10 Закону України «Про критичну інфраструктуру» Кабінет Міністрів України **постановляє:**

{Вступна частина із змінами, внесеними згідно з Постановою КМ № 1384 від 16.12.2022}

Затвердити такі, що додаються:

Порядок віднесення об’єктів до критичної інфраструктури;

{Абзац другий постановляючої частини в редакції Постанови КМ № 1384 від 16.12.2022}

перелік секторів критичної інфраструктури;

{Абзац третій постановляючої частини в редакції Постанови КМ № 1384 від 16.12.2022}

Методику категоризації об’єктів критичної інфраструктури.

Прем’єр-міністр України **Д. ШМИГАЛЬ**

Інд. 49

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 9 жовтня 2020 р. № 1109
(в редакції постанови Кабінету Міністрів України
від 16 грудня 2022 р. № 1384)

ПОРЯДОК
віднесення об’єктів до критичної інфраструктури

1. Цей Порядок визначає механізм віднесення об’єктів до критичної інфраструктури та їх категоризації.

Дія цього Порядку не поширюється на:

– банки, інші об’єкти, що провадять діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, платіжні

організації, учасників платіжних систем, операторів послуг платіжної інфраструктури, віднесення яких до критичної інфраструктури здійснюється в порядку, встановленому Національним банком;

– об’єкти, що провадять діяльність на ринках послуг, державне регулювання та нагляд за діяльністю яких здійснюють державні органи, віднесення яких до критичної інфраструктури здійснюється в порядку, встановленому такими державними органами.

2. Терміни в цьому Порядку вживаються у значенні, наведеному в Законі України «Про критичну інфраструктуру».

3. Категорії критичності об’єктів критичної інфраструктури установлюються відповідно до частини другої статті 10 Закону України «Про критичну інфраструктуру».

4. Секторальні органи у сфері захисту критичної інфраструктури, використовуючи перелік секторів критичної інфраструктури, ідентифікують об’єкти критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури.

5. Секторальні органи у сфері захисту критичної інфраструктури разом із оператором критичної інфраструктури здійснюють категоризацію об’єктів критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури відповідно до Методики категоризації об’єктів критичної інфраструктури, затвердженої постановою Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 «Деякі питання об’єктів критичної інфраструктури» (Офіційний вісник України, 2020 р., № 93, ст. 2994).

{Пункт 5 із змінами, внесеними згідно з Постановою КМ № 48 від 16.01.2024}

6. Відомості про об’єкти критичної інфраструктури, що віднесені до I, II, III і IV категорії критичності, вносяться секторальними органами у сфері захисту критичної інфраструктури до секторальних переліків об’єктів критичної інфраструктури, які ними складаються та ведуться.

7. Секторальні органи у сфері захисту критичної інфраструктури складають переліки об’єктів критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури, що віднесені до I, II, III і IV категорії критичності.

Секторальні органи у сфері захисту критичної інфраструктури подають уповноваженому органові у сфері захисту критичної інфраструктури переліки об’єктів критичної інфраструктури за формою згідно з додатком.

Секторальні органи у сфері захисту критичної інфраструктури подають оновлені секторальні переліки об’єктів критичної інфраструктури протягом 10 робочих днів з дня внесення до них змін.

Уповноважений орган у сфері захисту критичної інфраструктури має право ініціювати проведення повторної категоризації секторальним органом об’єкта критичної інфраструктури.

{Пункт 7 в редакції Постанови КМ № 48 від 16.01.2024}

8. Відомості про об’єкти критичної інфраструктури, що містяться у секторальних переліках об’єктів критичної інфраструктури, є інформацією з обмеженим доступом, захист якої забезпечується відповідно до вимог законодавства.

{Пункт 8 із змінами, внесеними згідно з Постановою КМ № 48 від 16.01.2024}

{Порядок в редакції Постанови КМ № 1384 від 16.12.2022}

Додаток до Порядку

СЕКТОРАЛЬНИЙ ПЕРЕЛІК
об’єктів критичної інфраструктури сектору

_____

(найменування сектору)

Порядковий номер	Сектор критичної нфраструктури	Підсектор критичної інфраструктури	Тип основної послуги	Найменування/ прізвище, ім’я, по батькові (у разі наявності) оператора критичної інфраструктури	Код згідно з ЄДРПОУ/ РНОКПП (у разі наявності) оператора критичної інфраструктури	Місцезнаходження/ адреса оператора критичної інфраструктури	Назва об’єктів критичної інфраструктури (стисла характеристика)	Місцезнаходження/ адреса об’єкта критичної інфраструктури	Категорія критичності об’єкта критичної інфраструктури	Узагальнена нормована оцінка рівня критичності

{Порядок доповнено додатком згідно з Постановою КМ № 48 від 16.01.2024}

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 9 жовтня 2020 р. № 1109
(в редакції постанови Кабінету Міністрів України
від 16 січня 2024 р. № 48)

ПЕРЕЛІК
секторів критичної інфраструктури

Сектор	Підсектор	Тип основної послуги	Секторальний орган у сфері захисту критичної інфраструктури
1. Паливно-енергетичний сектор	1) електроенергетика	виробництво електричної енергії	Міненерго
		забезпечення функціонування ринку електричної енергії, організація купівлі-продажу електричної енергії на ринку	
		управління системами передачі та енергопостачання	
		розподіл електричної енергії	
		експлуатація гідротехнічних споруд	

Сектор	Підсектор	Тип основної послуги	Секторальний орган у сфері захисту критичної інфраструктури
	2) вугільно-промисловий комплекс	видобуток вугілля для генерації електроенергії на теплоелектростанціях та теплоелектроцентралях	
		зберігання та постачання вугілля	
	3) торфодобування	розробка родовищ торфу	
		видобування корисних копалин	
	4) нафтова промисловість	видобуток нафти	
		передача (транзит) нафти та нафтопродуктів	
		очищення, переробка та обробка нафти	
		експлуатація нафтопроводів	
		зберігання та постачання нафти та нафтопродуктів	
	5) газова промисловість	видобуток газу	
		переробка та очищення газу	
		передача (транзит) газу	
		розподіл газу	
		забезпечення роботи систем зрідження природного газу	
		експлуатація газотранспортної системи	
		зберігання природного газу	
	6) ядерна енергетика	виробництво ядерного палива	
		експлуатація ядерних підкритичних установок, ядерних реакторів, які включають критичні та підкритичні збірки дослідницьких ядерних реакторів	
		експлуатація атомних електростанцій, підприємств і установок із збагачення та перероблення ядерного	
		палива, а також сховищ відпрацьованого ядерного палива	
		видобуток та переробка	

Сектор	Підсектор	Тип основної послуги	Секторальний орган у сфері захисту критичної інфраструктури
		уранової сировини	
	7) енергетичне машинобудування	виробництво високовольтного та низьковольтного електрообладнання, зокрема силових трансформаторів та реакторів для потреб енергетики	
2. Цифрові технології	1) електронні довірчі послуги та електронна ідентифікація	надання електронних довірчих послуг, послуг електронної ідентифікації	Мінцифри
		забезпечення функціонування інформаційно-комунікаційної системи центрального засвідчувального органу	
		забезпечення функціонування інтегрованої системи електронної ідентифікації	
	2) електронні комунікації	адміністрування адресного простору українського сегмента Інтернету	
		надання електронних комунікаційних послуг	
	3) електронне урядування	забезпечення функціонування системи електронної взаємодії органів виконавчої влади	
		забезпечення функціонування системи електронної взаємодії державних електронних інформаційних ресурсів «Трембіта»	
		забезпечення надання адміністративних послуг	
		забезпечення функціонування Єдиного державного вебпорталу електронних послуг та/або інших публічних електронних реєстрів та/або баз даних, національних	

Сектор	Підсектор	Тип основної послуги	Секторальний орган у сфері захисту критичної інфраструктури
		електронних інформаційних ресурсів, інформаційних (автоматизованих) систем, інформаційно-комунікаційних систем, ведення (функціонування) яких запроваджено нормативно-правовими актами	
3. Захист інформації		надання послуг (сервісів) кіберзахисту	Держспецзв'язку
4. Харчова промисловість та агропромисловий комплекс		виробництво та переробка сільськогосподарської та/або харчової продукції	Мінагрополітики
		виробництво ветеринарних препаратів	
		експлуатація елеваторів	
		експлуатація зрошувальних систем, каналів	
5. Державний матеріальний резерв		забезпечення зберігання запасів державного матеріального резерву	Мінекономіки
6. Охорона здоров'я	1) медична допомога	забезпечення надання екстреної медичної допомоги	МОЗ
		забезпечення надання первинної медичної допомоги	
		забезпечення надання спеціалізованої медичної допомоги	
		забезпечення надання паліативної медичної допомоги	
		забезпечення надання реабілітації у сфері охорони здоров'я	
	2) громадське здоров'я	заготівля і тестування донорської крові та компонентів крові	
		здійснення контролю за інфекційними захворюваннями та/або епідеміями	
	3) фінансове забезпечення у сфері	оплата згідно з тарифом за надані пацієнтам медичні	

Сектор	Підсектор	Тип основної послуги	Секторальний орган у сфері захисту критичної інфраструктури
	охорони здоров’я	послуги (включаючи медичні вироби) та лікарські засоби за договорами про медичне обслуговування населення за програмою медичних гарантій	
	4) інформаційні технології у сфері охорони здоров’я	функціонування електронної системи охорони здоров’я	
	5) фармацевтична промисловість	виробництво та забезпечення лікарськими засобами, медичними виробами	
7. Ринки капіталу та організовані товарні ринки		забезпечення функціонування ринків капіталів та організованих товарних ринків	НКЦПФР
8. Фінансовий сектор		планування, виконання та моніторинг виконання бюджетів	Мінфін
		розрахунково-касове обслуговування розпорядників та одержувачів бюджетних коштів	
		здійснення контролю за надходженням до бюджетів та державних цільових фондів податків, зборів, платежів	
		запобігання та протидія легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення	
		забезпечення функціонування системи гарантування вкладів фізичних осіб та виведення банків з ринку	
		здійснення контролю за надходженням митних платежів до державного	

Сектор	Підсектор	Тип основної послуги	Секторальний орган у сфері захисту критичної інфраструктури
		бюджету, валютного контролю, пропуск товарів, транспортних засобів через митний кордон України	
9. Транспорт і пошта	1) авіаційний транспорт	управління повітряним рухом	Мінінфраструктури
		авіаперевезення (робота авіаційного транспорту)	
		забезпечення роботи аеропортів та допоміжного обладнання, що розташоване в аеропортах	
	2) автомобільний та міський електричний транспорт	вантажні, автобусні перевезення (міжміські, міжнародні)	
		міські перевезення (автобуси, трамваї, тролейбуси)	
		нове будівництво, реконструкція, капітальний ремонт, послуги з поточного ремонту та експлуатаційного утримання автомобільних доріг та штучних споруд, що на них розміщені	
		служби контролю трафіка	
		функціонування інтелектуальних транспортних систем (управління рухом, мобільністю, взаємодія з іншими видами транспорту)	
		функціонування міжнародних, міждержавних та місцевих пунктів пропуску через державний кордон для автомобільного сполучення	
	3) метрополітен	перевезення пасажирів метрополітеном	
	4) залізничний транспорт	пасажирські залізничні перевезення	
		вантажні залізничні перевезення	
		експлуатація та технічне обслуговування залізниці	

Сектор	Підсектор	Тип основної послуги	Секторальний орган у сфері захисту критичної інфраструктури
		забезпечення роботи вокзалів та вузлових станцій	
	5) морський та внутрішній водний транспорт	здійснення контролю та нагляду за безпекою судноплавства та мореплавства	
		інжинірингова діяльність для будівництва, ефективного використання та утримання об’єктів портової інфраструктури, розташованих у межах території та акваторії морського порту	
		обслуговування суден, що заходять до морських, річкових портів (терміналів) України, пасажирів, вантажів (вантажно-розвантажувальні роботи, обслуговування, зберігання, перевезення вантажів, пасажирів)	
		обслуговування та утримання внутрішніх водних шляхів, об’єктів інфраструктури внутрішнього водного транспорту	
		виконання міжнародних зобов’язань України у тому числі: лоцманське проведення суден	
		регулювання руху суден	
		технічний нагляд за суднами	
		пошук і рятування людей в морі	
		гідрографічне забезпечення	
	6) поштовий зв’язок	надання послуг поштового зв’язку	
10. Системи життє-забезпечення	комунальні послуги	постачання теплової енергії	
		постачання гарячої води	
		централізоване питне водопостачання	
		централізоване водовідведення	
		управління побутовими	

Сектор	Підсектор	Тип основної послуги	Секторальний орган у сфері захисту критичної інфраструктури
		відходами	
11. Промисловість	1) хімічна промисловість	виробництво промислового газу	Мінстратегпром
		виробництво добрив або азотистих сполук	
		виробництво пестицидів або інших агрохімічних продуктів	
		виробництво вибухових речовин	
		виробництво основних органічних хімічних речовин	
		виробництво основних неорганічних речовин	
		зберігання небезпечних (особливо небезпечних) хімічних/вибухових речовин	
	2) металургійна промисловість	гірничо-металургійний комплекс (металургійне виробництво та добування залізних руд)	
		виробництво коксу та коксопродуктів	
	3) оборонна промисловість	розробка, виробництво, модернізація та утилізація продукції військового призначення; виробництво ракет, боєприпасів, вибухових речовин (оборонно-промислового комплексу)	
	4) космічна промисловість	виробництво та постачання космічної техніки	
		космічна діяльність, космічні технології та послуги	
	5) авіаційна промисловість	виробництво та постачання продукції авіаційної промисловості	
	6) суднобудівна промисловість	суднобудування та постачання продукції суднобудування	
12. Сектор громадської безпеки	1) громадська безпека	охорона публічного (громадського) порядку, охорона критичної	МВС

Сектор	Підсектор	Тип основної послуги	Секторальний орган у сфері захисту критичної інфраструктури
		інфраструктури, зокрема на договірних засадах	
	2) екстрена допомога населенню за єдиним телефонним номером 112	оперативне цілодобове невідкладне реагування на екстрені комунікації, їх оброблення, зберігання та передача інформації про такі комунікації для надання екстреної допомоги населенню за єдиним телефонним номером 112	
13. Цивільний захист населення і територій	служби порятунку (атестовані аварійно-рятувальні служби згідно із законодавством)	реагування на надзвичайні ситуації, проведення аварійно-рятувальних та інших невідкладних робіт з ліквідації наслідків надзвичайних ситуацій, надання допомоги постраждалим	
14. Охорона навколишнього природного середовища	1) управління, використання та відтворення поверхневих водних ресурсів, розвиток водного господарства	забезпечення задоволення потреб населення і галузей економіки у водних ресурсах	Міндовкілля
		проєктування, будівництво і реконструкція систем захисту від шкідливої дії вод, групових і локальних водопроводів, систем водопостачання та каналізації у сільській місцевості, гідротехнічних споруд, водогосподарських об’єктів багатоцільового використання	
		захист від підтоплення захисних масивів, протипаводковий і протиповеневий захист	
	2) поводження з радіоактивними відходами	довгострокове зберігання і захоронення радіоактивних відходів	
	3) охорона, раціональне використання і відтворення	охорона, раціональне використання земель та надр	
		охорона, раціональне використання і відтворення	

Сектор	Підсектор	Тип основної послуги	Секторальний орган у сфері захисту критичної інфраструктури
	об’єктів природно-заповідного фонду	об’єктів природно-заповідного фонду	
		ведення лісового і мисливського господарства	
		управління відходами, поводження з небезпечними хімічними речовинами, пестицидами та агрохімікатами	
		створення, дослідження та практичне використання генетично модифікованих організмів у відкритій системі	
15. Сектор оборони		оборона	Міноборони
	зберігання ракет, боєприпасів та вибухових речовин	зберігання ракет, боєприпасів та вибухових речовин	
		складання та ремонт боєприпасів та комплектувальних виробів до них	
16. Правосуддя		здійснення правосуддя	ДСА
17. Виконання кримінальних покарань, тримання під вартою та утримання військово-полонених		тримання засуджених, осіб, узятих під варту, в установах виконання покарань та слідчих ізоляторах Державної кримінально-виконавчої служби, а також утримання військовополонених у таборах (дільницях) для тримання військовополонених	Мін’юст
18. Державна реєстрація	інформаційні технології у сфері державної реєстрації	забезпечення функціонування інформаційної системи єдиних та державних реєстрів, держателем яких є Мін’юст	
19. Наукові дослідження та розробки	дослідницька інфраструктура наукових установ та закладів вищої освіти	наукова діяльність	МОН
		надання послуг з використання наукового обладнання (зокрема інструментів, приладів,	

Сектор	Підсектор	Тип основної послуги	Секторальний орган у сфері захисту критичної інфраструктури
		інвентарю)	
		дослідницька діяльність	
20. Фінансовий сектор	1) банківська система	надання банківських послуг	Національний банк
		зберігання банками запасів готівки Національного банку та проведення операцій із ними	
	2) ринок небанківських фінансових послуг (крім ринків капіталу та організованих товарних ринків)	надання електронних довірчих послуг у банківській системі	
		надання небанківських фінансових послуг	
	3) ринок платіжних послуг	надання платіжних послуг	
21. Вибори та референдуми		організація підготовки та проведення виборів та референдумів	Центральна виборча комісія
		функціонування інформаційних (автоматизованих), інформаційно-комунікаційних систем, електронних реєстрів, держателем чи розпорядником яких є Центральна виборча комісія	
22. Соціальний захист	1) пенсійне забезпечення	забезпечення пенсійних виплат	Мінсоцполітики
	2) соціальне страхування	надання матеріального забезпечення і страхових виплат	
	3) соціальна допомога і соціальні послуги	забезпечення соціальних виплат та/або надання соціальних послуг	
	4) інформаційна система соціальної сфери	надання адміністративних послуг соціального характеру в електронній формі	
	5) реабілітація	забезпечення допоміжними засобами реабілітації	
23. Інформаційний сектор	медіа	надання послуг у сфері телебачення та радіомовлення	МКІП
		надання послуг в	

Сектор	Підсектор	Тип основної послуги	Секторальний орган у сфері захисту критичної інфраструктури
		інформаційній та видавничій сфері	
24. Державна влада та місцеве самоврядування		виконання функцій держави	Секретаріат Кабінету Міністрів України
		виконання функцій місцевого самоврядування	

{Перелік із змінами, внесеними згідно з Постановами КМ № 1414 від 29.12.2021, № 991 від 02.09.2022; в редакції Постанови КМ № 1384 від 16.12.2022; із змінами, внесеними згідно з Постановою КМ № 455 від 09.05.2023; в редакції Постанови КМ № 48 від 16.01.2024}

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 9 жовтня 2020 р. № 1109

МЕТОДИКА
категоризації об’єктів критичної інфраструктури

1. Ця Методика визначає механізм та критерії віднесення об’єкта критичної інфраструктури до однієї з категорій критичності.

Дія цієї Методики не поширюється на:

{Пункт 1 доповнено абзацом згідно з Постановою КМ № 1384 від 16.12.2022}

– банківську та фінансову системи, категоризація об’єктів критичної інфраструктури яких здійснюється відповідно до методики, затвердженої Національним банком;

{Пункт 1 доповнено абзацом згідно з Постановою КМ № 1384 від 16.12.2022}

– сфери, державне регулювання та нагляд за діяльністю яких здійснюють державні органи, категоризація об’єктів критичної інфраструктури яких здійснюється відповідно до методики, затвердженої такими державними органами.

{Пункт 1 доповнено абзацом згідно з Постановою КМ № 1384 від 16.12.2022}

2. У цій Методиці під терміном «час відновлення» розуміється час, що необхідний для відновлення функціонування об’єкта критичної інфраструктури у частині надання основних послуг у штатному режимі після виникнення кризової ситуації, пошкодження або знищення об’єкта.

Інші терміни вживаються у значенні, наведеному в Законі України «Про критичну інфраструктуру».

{Пункт 2 в редакції Постанови КМ № 1384 від 16.12.2022}

3. Категорія критичності об’єкта критичної інфраструктури визначається на основі аналізу рівня негативного впливу, якого особа, суспільство, навколишнє природне середовище, економіка, національна безпека та обороноздатність країни можуть зазнати внаслідок порушення або припинення функціонування об’єкта інфраструктури відповідно до критеріїв, зазначених у додатках 1 і 2.

4. Категорія об’єкта критичної інфраструктури визначається за такою процедурою:

1) секторальний орган у сфері захисту критичної інфраструктури ідентифікує всі об’єкти критичної інфраструктури свого сектору (підсектору) критичної інфраструктури згідно з Порядком віднесення об’єктів до критичної інфраструктури, затвердженим постановою Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 «Деякі питання об’єктів критичної інфраструктури» (Офіційний вісник України, 2020 р., № 93, ст. 2994), – в редакції постанови Кабінету Міністрів України від 16 грудня 2022 р. № 1384;

{Підпункт 1 пункту 4 із змінами, внесеними згідно з Постановою КМ № 1384 від 16.12.2022}

2) секторальний орган у сфері захисту критичної інфраструктури відповідно до Порядку віднесення об’єктів до критичної інфраструктури для кожного об’єкта свого сектору (підсектору) критичної інфраструктури визначає, які основні послуги надає цей об’єкт;

{Підпункт 2 пункту 4 із змінами, внесеними згідно з Постановою КМ № 1384 від 16.12.2022}

3) секторальний орган у сфері захисту критичної інфраструктури разом із оператором критичної інфраструктури проводить оцінку критичності об’єкта критичної інфраструктури, використовуючи секторальні та міжсекторальні критерії визначення рівня негативного впливу, наведені у додатках 1 і 2, які враховують:

{Абзац перший підпункту 3 пункту 4 із змінами, внесеними згідно з Постановою КМ № 1384 від 16.12.2022}

– рівень негативного впливу на надання основних послуг у разі знищення,

пошкодження або порушення функціонування об’єкта критичної інфраструктури;

– соціальну значущість об’єкта критичної інфраструктури;

– суспільну значущість об’єкта критичної інфраструктури;

– економічну значущість об’єкта критичної інфраструктури;

– наявність взаємозв’язків між об’єктами критичної інфраструктури;

– значущість об’єкта критичної інфраструктури для забезпечення національної безпеки та обороноздатності країни;

4) під час заповнення форми додатка 1 обирається рівень негативного впливу в рамках сектору або підсектору об’єкта критичної інфраструктури та у графі «Оцінка РК» виставляється бал, який відповідає рівню негативного впливу, опис якого характеризує наслідки, які можуть настати у разі порушення функціонування об’єкта критичної інфраструктури;

5) під час заповнення форми додатка 2 обирається рівень негативного впливу за кожним критерієм, наведеним у формі, та у графі «Оцінка РК» виставляється бал, який відповідає рівню негативного впливу, опис якого характеризує наслідки, які можуть настати у разі порушення функціонування об’єкта критичної інфраструктури;

6) підсумовуються всі бали, що були отримані під час оцінки об’єкта критичної інфраструктури згідно з формами, наведеними в додатках 1 і 2;

7) розраховується узагальнена нормована оцінка рівня критичності за такою формулою:

де $РК_{окі}$ – узагальнена нормована оцінка рівня критичності об’єкта критичної інфраструктури; – сума балів, які отримав об’єкт критичної інфраструктури за всіма критеріями критичності (додатки 1 і 2); – - максимальна можлива сума балів (розраховується виходячи з того, що об’єкт отримує максимальні бали за всіма критеріями оцінки рівня негативного впливу).
Примітка. У цій Методиці залежно від сектору використовується 17 або 18 критеріїв, тому для об’єктів критичної інфраструктури, що належать до секторів критичної інфраструктури згідно з пунктами 1 і 3, 5 і 6, 8-10, 22, 25 і 26, 29 і 30 додатка 1, максимальна можлива сума балів буде дорівнювати $\sum РК_{max} = 18 \times 4 = 72$ бали. Для об’єктів критичної інфраструктури, що належать до секторів згідно з пунктами 2 і 4, 7, 11-21, 23 і 24, 27 і 28, 31-33 додатка 1, максимальна можлива сума балів буде дорівнювати $\sum РК_{max} = 17 \times 4 = 68$ балів.

{Підпункт 7 пункту 4 із змінами, внесеними згідно з Постановою КМ № 48 від 16.01.2024}

8) рішення щодо категорії критичності об’єкта критичної інфраструктури приймається на основі узагальненої нормованої оцінки рівня критичності об’єкта критичної інфраструктури відповідно до такого правила:

I категорія критичності, якщо $0,8 < РК_{окі} \leq 1$;

II категорія критичності, якщо $0,63 < РК_{окі} \leq 0,8$;

III категорія критичності, якщо $0,37 < РК_{окі} \leq 0,63$;

IV категорія критичності, якщо $0,2 < РК_{окі} \leq 0,37$;

об’єкт не є критичним, якщо $РК_{окі} \leq 0,2$;

{Підпункт 9 пункту 4 виключено на підставі Постанови КМ № 48 від 16.01.2024}

10) відомості про об’єкти критичної інфраструктури, що віднесені до I, II, III і IV категорії критичності, вносяться до секторального переліку об’єктів критичної інфраструктури,

який формується та ведеться секторальним органом у сфері захисту критичної інфраструктури у відповідному секторі (підсекторі).

{Підпункт 10 пункту 4 в редакції Постанови КМ № 1384 від 16.12.2022}

5. Методичні рекомендації щодо категоризації об'єкта критичної інфраструктури затверджує Адміністрація Держспецзв'язку.

Додаток 1 до Методики
(в редакції постанови Кабінету Міністрів України
від 16 січня 2024 р. № 48)

ВИЗНАЧЕННЯ РІВНЯ
негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури (секторальні критерії)

Сектор/ підсектор		Фактор негативного впливу в секторі/ підсекторі	Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бали)	Рівень негативного впливу: незначні наслідки (1 бал)	Оцінка $\sum РК_i$
1.	Послуги, що надаються підсектором електроенергетики та підсектором ядерної енергетики	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення електропостачання	для більше ніж 145 000 жителів або для споживачів I категорії на території більше ніж однієї області або на території не менше ніж 3 міст обласного значення	для більше ніж 30 000 жителів або для споживачів II категорії на території однієї області або на території більше ніж 1 району міста – обласного центру, або на всій території одного міста обласного значення	для більше ніж 2000 жителів	для менше ніж 2000 жителів	
			час відновлення функціонування у штатному режимі не може перевищувати 6 годин	час відновлення функціонування у штатному режимі може становити від 6 до 24 годин	час відновлення функціонування у штатному режимі може становити від 1 до 3 діб	час відновлення функціонування у штатному режимі може становить більше 3 діб	
2.	Послуги, що надаються підсектором енергетичного машинобудування	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення виробництва та надання послуг з ремонту силових трансформаторів та реакторів	для більше ніж 145 000 жителів на території більше ніж однієї області або не менше ніж 3 міст обласного значення	для більше ніж 30 000 жителів на території області або більше ніж 1 району міста – обласного центру, або на всій території одного міста обласного значення	для більше ніж 6000 жителів	не застосовується	

Сектор/ підсектор		Фактор негативного впливу в секторі/ підсекторі	Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бали)	Рівень негативного впливу: незначні наслідки (1 бал)	Оцінка $\sum РК_i$
3.	Послуги, що надаються підсектором вугільно-промислового комплексу та підсектором торфо-добування	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення видобутку вугілля або торфу, постачання на об'єкти генерації (теплоелектро-станціях та теплоелектро-централях)	для більше ніж 30 000 жителів на території однієї області або на території більше ніж 1 району міста – обласного центру, або на всій території одного міста	для більше ніж 10 000 жителів	для більше ніж 5000 жителів	для менше ніж 5000 жителів	
			час відновлення функціонування у штатному режимі не може перевищувати 6 годин	час відновлення функціонування у штатному режимі може становити від 6 до 24 годин	час відновлення функціонування у штатному режимі може становити від 1 до 3 діб	час відновлення функціонування у штатному режимі може становить більше 3 діб	
4.	Послуги, що надаються підсектором нафтової промисловості	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до зменшення обсягів постачання нафти та нафтопродуктів для споживання на внутрішньому ринку	більше ніж на 25 % порівняно з аналогічним періодом календарного року чи попереднього календарного місяця	від 12 до 25 % порівняно з аналогічним періодом календарного року чи попереднього календарного місяця	від 7 до 12 % порівняно з аналогічним періодом календарного року чи попереднім календарним місяцем	менше ніж на 7 % порівняно з аналогічним періодом календарного року чи попереднім календарним місяцем	
5.	Послуги, що надаються підсектором газової промисловості	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення постачання газу	для більше ніж 145 000 жителів або для споживачів з безперервною подачею газу на території більше ніж 1 області або на території не менше ніж 3 міст обласного значення	для більше ніж 20 000 жителів на території однієї області або на території більше ніж 1 району міста – обласного центру, або на всій території 1 міста обласного значення	для більше ніж 5000 жителів	для менше ніж 5000 жителів	
			час відновлення функціонування у штатному	час відновлення функціонування у штатному режимі	час відновлення функціонування у штатному	час відновлення функціонування у штатному	

Сектор/ підсектор		Фактор негативного впливу в секторі/ підсекторі	Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бали)	Рівень негативного впливу: незначні наслідки (1 бал)	Оцінка $\sum РК_i$
			режимі не може перевищувати 6 годин	може становити від 6 до 24 годин	режимі може становити від 1 до 3 діб	режимі може становить більше 3 діб	
6.	Послуги, що надаються інформаційним сектором та сектором цифрових технологій	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення або зменшення обсягу надання основних послуг об'єктом	для більше ніж 145 000 жителів на території більше ніж 1 області або на території не менше ніж 3 міст обласного значення	для більше ніж 20 000 жителів на території однієї області або на території більше ніж 1 району міста – обласного центру, або на всій території одного міста обласного значення	для більше ніж 2000 жителів	для менше ніж 2000 жителів	
			час відновлення функціонування у штатному режимі не може перевищувати 6 годин	час відновлення функціонування у штатному режимі може становити від 6 до 24 годин	час відновлення функціонування у штатному режимі може становити від 1 до 3 діб	час відновлення функціонування у штатному режимі може становить більше 3 діб	
7.	Послуги, що надаються підсектором електронних комунікацій	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення або зменшення обсягу надання основних послуг	втрата можливості функціонування елементів електронної комунікаційної мережі або мережевої інфраструктури або інфраструктури центру обробки даних чи обміну трафіком для України або значної її частини	збій, переривання у наданні основних послуг або обмеження доступу користувачам послуг чи сервісів для великих міст чи цілих регіонів	відсутність стабільного з'єднання, переривання сесій, зниження пропускної здатності електронних комунікаційних мереж для операторів або частини користувачів	не застосовується	
8.	Послуги з постачання теплової енергії та гарячої води	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення постачання теплової енергії та/або гарячої води буде перервано (під час опалювального сезону)	для більше ніж 145 000 жителів або на території більше ніж 1 області, або не менше ніж 3 міст обласного значення	для більше ніж 30000 жителів або на території більше ніж одного району міста – обласного центру, або на всій території одного міста обласного значення	для більше ніж 2000 жителів	для менше ніж 2000 жителів	
			час відновлення функціонування у штатному режимі не може	час відновлення функціонування у штатному режимі може становити від	час відновлення функціонування у штатному режимі може	не застосовується	

Сектор/ підсектор		Фактор негативного впливу в секторі/ підсекторі	Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бали)	Рівень негативного впливу: незначні наслідки (1 бал)	Оцінка $\sum РК_i$
			перевищувати 24 годин	доби до 3 діб	становити від 3 діб		
9.	Послуги з централізованого питного водопостачання	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення централізованого водопостачання	для більше ніж 145 000 жителів або на території більше ніж 1 області, або не менше ніж 3 міст обласного значення	для більше ніж 30000 жителів або стаціонарним лікувальним закладам, будинкам соціальної допомоги, установам, що надають послуги освіти на території області або більше ніж 1 району міста – обласного центру, або на всій території одного міста обласного значення	для більше ніж 2000 жителів	для менше ніж 2000 жителів	
			час відновлення функціонування у штатному режимі не може перевищувати 24 годин (час кризової ситуації не може перевищувати 24 годин)	час відновлення функціонування у штатному режимі може становити від доби до трьох діб (час кризової ситуації може становити від 1 до 3 діб)	час відновлення функціонування у штатному режимі може становити від 1 до 3 діб (час кризової ситуації може становити від 1 до 3 діб)	не застосовується	
10.	Послуги з централізованого водовідведення	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення централізованого водовідведення та очищення стічних вод	для більше ніж 145 000 жителів або на території обласного центру, або не менше ніж 3 міст обласного значення	для більше ніж 30 000 жителів або на території одного міського району обласного центру, або на всій території 1 міста обласного значення	для більше ніж 2000 жителів	для менше ніж 2000 жителів	
			час відновлення функціонування у штатному режимі не може перевищувати 24 годин (час кризової ситуації не може перевищувати 24 годин)	час відновлення функціонування у штатному режимі може становити від 1 до 3 діб (час кризової ситуації може становити від 1 до 3 діб)	час відновлення функціонування у штатному режимі може становити від 1 до 3 діб (час кризової ситуації може становити від 1 до 3 діб)	не застосовується	
11.	Послуги з управління побутовими відходами	знищення, пошкодження або порушення функціонування об'єкта критичної	для більше ніж 145 000 жителів або на території обласного центру, або не	для більше ніж 30 000 жителів або на території одного міського району обласного центру,	не застосовується	не застосовується	

Сектор/ підсектор		Фактор негативного впливу в секторі/ підсекторі	Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бали)	Рівень негативного впливу: незначні наслідки (1 бал)	Оцінка $\sum РК_i$
		інфраструктури призведе до припинення збору, зберігання, безпечної переробки (утилізації) побутових відходів	менше ніж трьох міст обласного значення	або на всій території 1 міста обласного значення			
12.	Послуги, що надаються підсектором авіаційного транспорту	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури	неможливість надання послуг з перевезення пасажирів та вантажів авіаційним транспортом (хоча б одним із стратегічно важливих аеропортів України) протягом більше ніж 24 годин без можливості організації альтернативного способу надання послуг	неможливість надання послуг з перевезення пасажирів та вантажів авіаційним транспортом (хоча б одним із стратегічно важливих аеропортів України) протягом більше ніж 24 годин з можливістю організації альтернативного способу надання послуги	припинення повітряного руху на час відновлення штатного режиму функціонування	не застосовується	
13.	Послуги, що надаються підсектором авто-мобільного транспорту	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури	блокування (припинення) дорожнього руху на мостах, шляхопроводах, міжнародних та національних дорогах більше ніж на 24 години за відсутності обхідного шляху або відсутність можливості його відновлення протягом не більше ніж 24 годин	блокування (припинення) дорожнього руху на мостах, шляхопроводах, міжнародних та національних дорогах не більше ніж на 24 години за відсутності обхідного шляху	блокування (припинення) дорожнього руху на мостах, шляхопроводах, регіональних дорогах протягом не більше ніж на 48 годин за відсутності обхідного шляху або відсутності можливості його відновлення протягом не більше ніж 48 годин	блокування (припинення) дорожнього руху на мостах, шляхопроводах, регіональних дорогах протягом не більше ніж на 48 годин за відсутності обхідного шляху	
14.	Послуги, що надаються підсектором залізничного транспорту	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури	припинення залізничного руху на залізничних магістральних лініях I (I-П, I-ПС)	припинення залізничного руху на залізничних магістральних лініях III категорії (ДБН В.2.3-19-2018)	припинення залізничного руху на залізничних магістральних лініях IV	припинення залізничного руху на залізничних магістральних лініях V	

Сектор/ підсектор		Фактор негативного впливу в секторі/ підсекторі	Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бали)	Рівень негативного впливу: незначні наслідки (1 бал)	Оцінка $\sum РК_i$
			та II категорій (ДБН В.2.3-19-2018) за часом, що перевищує 24 години, за відсутності можливості забезпечення руху обхідною залізничною лінією або суміжною колією, а також через штучні споруди (мости, шляхопроводи, віадуки, тунелі), розташовані на залізничній магістральній лінії від кордонів з країнами Європейського Союзу до найближчої вузлової станції, та інші мости повною довжиною понад 1000 метрів	за часом, що перевищує 24 години, за відсутності можливості забезпечення руху обхідною залізничною лінією або через суміжною колією, а також через штучні споруди (мости, шляхопроводи, віадуки, тунелі), розташовані на залізничній магістральній лінії від кордонів з країнами Європейського Союзу до найближчої вузлової станції, та інші мости повною довжиною понад 1000 метрів	категорії (ДБН В.2.3-19-2018) за часом, що перевищує 24 години, за відсутності можливості забезпечення руху обхідною залізничною лінією або суміжною колією, а також через штучні споруди (мости, шляхопроводи, віадуки, тунелі), які розташовані на залізничній магістральній лінії від кордонів з країнами Європейського Союзу до найближчої вузлової станції, та інші мости повною довжиною понад 1000 метрів	категорії (ДБН В.2.3-19-2018) за часом, що перевищує 24 години, за відсутності можливості забезпечення руху обхідною залізничною лінією або суміжною колією, а також через штучні споруди (мости, шляхопроводи, віадуки, тунелі), які розташовані на залізничній магістральній лінії від кордонів з країнами Європейського союзу до найближчої вузлової станції, та інші мости повною довжиною понад 1000 метрів	
15.	Послуги, що надаються підсектором морського та внутрішнього водного транспорту	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури	припинення надання морських послуг у морських портах більше ніж на 72 годин (Правила надання послуг у морських портах України, затверджені наказом Мінінфра-структури від 05.06.2013 р. № 348)	час припинення надання морських послуг у морських портах може становити від 24 до 72 годин	час припинення надання морських послуг у морських портах може становити не більше ніж 24 години	не застосовується	
16.	Послуги, що надаються підсектором метрополітену	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури	припинення надання послуг з перевезення пасажирів більше ніж на 45 % загальних пасажирських	припинення надання послуг більше ніж 15 % загальних пасажирських перевезень міста або на території, що охоплює більше 25 %	припинення надання послуг більше ніж 5 % загальних пасажирських перевезень міста або на	припинення надання послуг до 5 % загальних пасажирських перевезень міста або на території, що	

Сектор/ підсектор		Фактор негативного впливу в секторі/ підсекторі	Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бали)	Рівень негативного впливу: незначні наслідки (1 бал)	Оцінка $\sum РК_i$
			перевезень міста або на території, що охоплює більше 50 % районів міста	районів міста	території, що охоплює більше 10 % районів міста	охоплює до 10 % районів міста	
17.	Послуги із збереження функціо-нування міждержавних та місцевих пунктів пропуску через державний кордон для авто-мобільного сполучення	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до ненадання об'єктом основних послуг	блокування (припинення) роботи міжнародних, міждержавних та місцевих пунктів пропуску через державний кордон для автомобільного сполучення більше ніж на 24 години за відсутності можливості відновлення його роботи протягом не більше ніж 24 годин	блокування (припинення) роботи міжнародних та міждержавних пунктів пропуску через державний кордон для автомобільного сполучення не більше ніж на 24 години за відсутності альтернативного способу надання послуг	блокування (припинення) роботи місцевих пунктів пропуску через державний кордон для автомобільного сполучення протягом не більше ніж на 48 годин за відсутності можливості відновлення його роботи протягом не більше ніж 48 годин	блокування (припинення) роботи місцевих пунктів пропуску через державний кордон для автомобільного сполучення протягом не більше ніж на 48 годин за відсутності альтернативного способу надання послуг	
18.	Послуги, що надаються підсектором поштового зв'язку	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення надання послуг поштового зв'язку	для більше ніж 145 000 жителів на території більше однієї області або більше ніж 3 міст обласного значення	для більше ніж 20 000 жителів на території області або більше одного району міста – обласного центру, або на всій території одного міста обласного значення	для більше ніж 6000 жителів	для менше ніж 6000 жителів	
19.	Послуги, що надаються сектором промисловості	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до ненадання об'єктом основних послуг	для більше ніж 100 000 жителів на території більше ніж 1 області або не менше ніж 3 міст обласного значення	для більше ніж 30 000 жителів на території області або більше ніж 1 району міста – обласного центру, або на всій території 1 міста обласного значення	для більше ніж 6000 жителів	для менше ніж 6000 жителів	
20.	Послуги, що надаються фінансовим сектором	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до ненадання	для більше ніж 100 000 клієнтів	для більше ніж 50 000 клієнтів	для більше ніж 10 000 клієнтів	не застосовується	

Сектор/ підсектор		Фактор негативного впливу в секторі/ підсекторі	Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бали)	Рівень негативного впливу: незначні наслідки (1 бал)	Оцінка $\sum РК_i$
		об'єктом основних послуг					
21.	Послуги, що надаються сектором харчової промисловості та агропро-мислового комплексу, сектором охорони навколишнього природного середовища, сектором охорони здоров'я, сектором цивільного захисту населення та територій, сектором соціального захисту	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до ненадання об'єктом основних послуг	для більше ніж 145 000 жителів на території більше ніж 1 області або не менше ніж 3 міст обласного значення	для більше ніж 30 000 жителів на території області або більше ніж 1 району міста – обласного центру, або на всій території 1 міста обласного значення	для більше ніж 6000 жителів	для менше ніж 6000 жителів	
22.	Послуги, що надаються сектором державного матеріального резерву (зберігання запасів державного матеріального резерву)	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до ненадання об'єктом основних послуг	для більше ніж 145 000 жителів або для споживачів I категорії на території більше ніж 1 області або не менше ніж 3 міст обласного значення	для більше ніж 30 000 жителів або для споживачів II категорії на території області або більше ніж 1 району міста – обласного центру, або на всій території одного 1 обласного значення	для більше ніж 2000 жителів	для менше ніж 2000 жителів	
			час відновлення функціонування у штатному режимі не може перевищувати 6 годин	час відновлення функціонування у штатному режимі може становити від 6 до 24 годин	час відновлення функціонування у штатному режимі може становити від 1 до 3 діб	час відновлення функціонування у штатному режимі може становити більше 3 діб	
23.	Послуги, що надаються сектором громадської безпеки	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до ненадання об'єктом основних послуг	для більше ніж 145 000 жителів або на території більше ніж 1 області, або не менше ніж 3 міст обласного значення	для більше ніж 30000 жителів або на території більше ніж 1 району міста обласного центру, або на всій території 1 міста обласного значення	для більше ніж 2000 абонентів	для менше ніж 2000 абонентів	

Сектор/ підсектор		Фактор негативного впливу в секторі/ підсекторі	Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бали)	Рівень негативного впливу: незначні наслідки (1 бал)	Оцінка $\sum РК_i$
24.	Послуги, що надаються підсектором екстреної допомоги населенню за єдиним телефонним номером 112	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення оперативного цілодобове невідкладного реагування на екстрені комунікації, їх оброблення, зберігання та передача інформації про такі комунікації для надання допомоги населенню за єдиним телефонним номером 112	для більше ніж 145 000 жителів або на території більше ніж 1 області, або не менше ніж 3 міст обласного значення	для більше ніж 30000 жителів або на території більше ніж 1 району міста обласного центру, або на всій території 1 міста обласного значення	для більше ніж 2000 абонентів	для менше ніж 2000 абонентів	
25.	Послуги, що надаються сектором правосуддя	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури	на всій території України	на території однієї або декількох областей	на території району області або району міста	не застосовується	
			припинення надання послуг за відсутності можливості невідкладно організувати альтернативний спосіб їх надання			припинення надання послуг за відсутності можливості невідкладно організувати альтернативний спосіб їх надання	
26.	Послуги, що надаються сектором «Вибори та референдуми»	знищення, пошкодження або порушення функціонування об'єкта інфраструктури призведе до неможливості організації підготовки та проведення виборів чи референдуму	неможливість здійснення суб'єктами виборчого процесу/ процесу референдуму виборчих процедур/ процедур референдуму на загальнодержавних	неможливість здійснення суб'єктами виборчого процесу/ процесу референдуму виборчих процедур/ процедур референдуму на місцевих виборах/ місцевому референдумі без можливості організації альтернативного способу здійснення відповідних процедур	відсутність можливості здійснення суб'єктами виборчого процесу/процесу референдуму виборчих процедур/ процедур референдуму за наявності можливості	неможливість здійснення суб'єктами виборчого процесу/процесу референдуму виборчих процедур/ процедур референдуму, що не впливає на надання основної	

Сектор/ підсектор		Фактор негативного впливу в секторі/ підсекторі	Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бали)	Рівень негативного впливу: незначні наслідки (1 бал)	Оцінка $\sum РК_i$
		відповідно до вимог закону	виборах/всеукраїнському референдумі без можливості організації альтернативного способу здійснення відповідних процедур у межах встановленого законодавством строку	у межах встановленого законодавством строку	організації альтернативного способу здійснення відповідних процедур у межах встановленого законодавством строку	послуги	
			час відновлення функціонування у штатному режимі не може перевищувати встановлений законодавством строк здійснення відповідних процедур на загальнодержавних виборах/ всеукраїнському референдумі без можливості організації альтернативного способу їх здійснення	час відновлення функціонування у штатному режимі не може перевищувати встановлений законодавством строк здійснення відповідних процедур на місцевих виборах/ місцевому референдумі без можливості організації альтернативного способу їх здійснення	час відновлення функціонування у штатному режимі не може перевищувати встановлений законодавством строк здійснення відповідних виборчих процедур/ процедур референдуму за наявності можливості організації альтернативного способу їх здійснення	час відновлення функціонування у штатному режимі може перевищувати встановлений законодавством строк здійснення відповідних виборчих процедур/ процедур референдуму	
27.	Послуги оборони	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до ненадання об'єктом основних послуг	для жителів на території більше ніж 2-3 областей або не менше ніж 1 області	для жителів на території більше ніж 1 області або не менше ніж 3 міст обласного значення	для жителів на території області або більше ніж 1 району міста – обласного центру, або на всій території 1 міста обласного значення	для жителів більше ніж 1 району області або на всій території 1 міста районного значення	
28.	Послуги, що надаються підсектором зберігання ракет, боєприпасів та вибухових речовин	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до ненадання об'єктом основних послуг	для забезпечення боєприпасами військових частин на території більше ніж 3 областей	для забезпечення боєприпасами військових частин на території 2 областей або не менше 1 області	для забезпечення боєприпасами військових частин на території 1 області або не менше 3 районів області	для забезпечення боєприпасами військових частин 2-3 районів області	
29.	Послуги, що надаються сектором	знищення, пошкодження або порушення	для більше ніж 145 000 жителів на території	для більше ніж 20 000 жителів на території області або більше	для більше ніж 5000 жителів	для менше ніж 5000 жителів	

Сектор/ підсектор		Фактор негативного впливу в секторі/ підсекторі	Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бали)	Рівень негативного впливу: незначні наслідки (1 бал)	Оцінка $\sum РК_i$
	виконання кримінальних покарань, тримання під вартою та утримання військово-полонених	функціонування об'єкта критичної інфраструктури призведе до ненадання об'єктом основних послуг	більше ніж 1 області або не менше ніж 3 міст обласного значення	1 району міста – обласного центру, або на всій території 1 міста обласного значення			
			припинення надання послуг з виконання кримінальних покарань, попереднього ув'язнення та тримання військово-полонених більше ніж на 72 години	припинення надання послуг з виконання кримінальних покарань, попереднього ув'язнення та тримання військовополонених може становити від 48 до 72 годин	припинення надання послуг з виконання кримінальних покарань, попереднього ув'язнення та тримання військово-полонених може становити від 24 до 48 годин	припинення надання послуг з виконання кримінальних покарань, попереднього ув'язнення та тримання військово-полонених може становити від 24 до 48 годин	
30.	Послуги, що надаються сектором ринків капіталу та організованих товарних ринків	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення або порушення надання об'єктом основних послуг	для більше ніж 25 000 учасників ринку капіталу та їх клієнтів	для більше ніж 10 000 учасників ринку капіталу та їх клієнтів	для більше ніж 5 000 учасників ринку капіталу та їх клієнтів	не застосовується	
			час відновлення функціонування у штатному режимі не може перевищувати 6 годин	час відновлення функціонування у штатному режимі може становити від 6 до 24 годин	час відновлення функціонування у штатному режимі може становити від 1 до 3 діб	час відновлення функціонування у штатному режимі може становити більше 3 діб	
31.	Послуги, що надаються сектором наукових досліджень та розробок	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до припинення виконання досліджень, зокрема тих, що виконуються для сектору безпеки та	неможливість надання послуг з проведення наукових досліджень, які здійснюються за замовленням держави для важливих секторів економіки та безпеки, а також за міжнародними	втрата унікального наукового обладнання, яке забезпечує надання послуг з проведення наукових досліджень, які здійснюються за замовленням держави для важливих секторів економіки та безпеки, а також за міжнародними договорами, укладеними від імені України	неможливість надання послуг з проведення наукових досліджень співвиконавцем наукових досліджень, які здійснюються за замовленням держави для важливих секторів економіки та	не застосовується	

Сектор/ підсектор		Фактор негативного впливу в секторі/ підсекторі	Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бали)	Рівень негативного впливу: незначні наслідки (1 бал)	Оцінка $\sum РК_i$
		оборони з міжнародними договорами, укладеними від імені України	договорами, укладеними від імені України		безпеки, а також за міжнародними договорами, укладеними від імені України		
32.	Послуги, що надаються сектором державної влади та місцевого самовря-дування	знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури призведе до ненадання об'єктом основних послуг	для жителів на території всієї країни	для жителів на території 1 області	для жителів на території територіальної громади	для жителів на території 1 району міста обласного значення	
33.	Послуги (сервіси) кіберзахисту	у разі знищення або пошкодження, порушення сталого функціонування об'єкта критичної інфраструктури	припинення надання послуг, які надаються на національному рівні (2 і більше) центральним органам виконавчої влади, державним органам, Національному банку та об'єктам критичної інфраструктури I категорії критичності	припинення надання послуг, які надаються на регіональному/ міжрегіональному, галузевому/ міжгалузевому рівні центральному органу виконавчої влади, визначеним відповідальними за забезпечення формування та реалізацію державної політики у сфері захисту критичної інфраструктури в окремому секторі, центральному органу виконавчої влади, 2 та більше місцевим держадміністраціям (військово-цивільним адміністраціям – у разі створення), 2 та більше місцевим органам виконавчої влади, об'єктам критичної інфраструктури II категорії критичності	наслідком є припинення надання послуг, які надаються на місцевому рівні органу виконавчої влади (військово-цивільній адміністрації – у разі створення), органу місцевого самоврядування, об'єктам критичної інфраструктури III, IV категорії критичності	припинення надання послуг операторам критичної інфраструктури на об'єктовому рівні	

{Додаток 1 із змінами, внесеними згідно з Постановою КМ № 1384 від 16.12.2022; в редакції Постанови КМ № 48 від 16.01.2024}

Додаток 2 до Методики

ВИЗНАЧЕННЯ РІВНЯ
негативного впливу у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури (міжсекторальні критерії)

	Негативний вплив	Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бали)	Рівень негативного впливу: незначні наслідки (1 бал)	Рівень негативного впливу: надто малий (0 балів)	Оцінка РКі
І. Соціальна значущість об'єкта критичної інфраструктури							
1.	Заподіяння шкоди життю та здоров'ю людей	*Кількість населення, що може постраждати*					
		небезпека для життя або здоров'я більше ніж 75 000 людей	небезпека для життя та здоров'я більше ніж 5000 людей	небезпека для життя або здоров'я більше ніж 50 людей	небезпека для життя або здоров'я менше ніж 50 людей	не критично	$РК_1$ =
		Географічний масштаб					
		небезпека для життя та здоров'я мешканців на території 1 або більше ніж 1 області, або на території 3 та більше міст обласного значення	небезпека для життя та здоров'я мешканців на території 1 області або міського району міста обласного центру, або на всій території 1 міста обласного значення	небезпека для життя та здоров'я для людей на території об'єкта та для мешканців, що проживають у безпосередній близькості до розміщення об'єкта	небезпека для життя та здоров'я людей на території об'єкта	не критично	$РК_2$ =
2.	Заподіяння шкоди навколишньому природному середовищу	*Економічні втрати*					
		нанесені збитки більше ніж 30 млн грн	нанесені збитки більше ніж 18 млн грн	нанесені збитки більше ніж 2 млн грн	нанесені збитки менше ніж на 2 млн грн	не критично	$РК_3$ =
		Географічний масштаб					
		шкідливий вплив поширюється на територію більше ніж однієї області або на території не менше ніж 3 міст обласного значення	шкідливий вплив поширюється на територію однієї області або на територію більше ніж 1 міста обласного значення	шкідливий вплив поширюється на територію 1 міста обласного значення	шкідливий вплив поширюється на територію об'єкта інфраструктури	не критично	$РК_4$ =
		Час					
		шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом більше ніж 1 року	шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом від півроку до 1 року	шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом від 1 місяця до півроку	шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом 1 місяця	не критично	$РК_5$ =

Негативний вплив		Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бали)	Рівень негативного впливу: незначні наслідки (1 бал)	Рівень негативного впливу: надто малий (0 балів)	Оцінка РКі
ІІ. Суспільна значущість об'єкта критичної інфраструктури							
3.	Припинення або порушення функціонування державних органів	припинення або порушення функціонування Верховної Ради України, Кабінету Міністрів України, Конституційного Суду України, Верховного Суду, а також Офісу Президента України, Ради національної безпеки та оборони України	припинення або порушення функціонування центральних органів виконавчої влади та облдержадміністрацій	припинення або порушення роботи районних держадміністрацій, територіальних органів центральних органів виконавчої влади	припинення або порушення роботи органів місцевого самоврядування	не критично	$РК_6$ =
4.	Негативний вплив на довіру людей до державних інституцій	матиме значний вплив				не критично	$РК_7$ =
5.	Шкода інтересам інших держав-партнерів України	так, принаймні 2 країнам або порушення умов міжнародного договору, укладеного від імені України	так, принаймні 1 країні або порушення умов міжнародного договору, укладеного від імені Уряду України	можливі негативні наслідки для інших держав, але їх вплив навряд чи буде значним	держави не постраждають або не має місце порушення умов міжнародного договору, укладеного від імені міністерства, іншого центрального органу виконавчої влади, державного органу	не критично	$РК_8$ =
ІІІ. Економічна значущість об'єкта критичної інфраструктури							
6.	Заподіяння збитків оператору критичної інфраструктури (у відсотках прогнозованого обсягу річного доходу за всіма видами діяльності)	більше ніж 15 %	від 10 до 15 %	від 5 до 10 %	менше ніж 5 %	не критично	$РК_9$ =

Негативний вплив		Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бали)	Рівень негативного впливу: незначні наслідки (1 бал)	Рівень негативного впливу: надто малий (0 балів)	Оцінка РКі
7.	Заподіяння збитків державному бюджету (зниження прибутків бюджету у відсотках прогнозованого річного прибутку бюджету)	більше ніж 0,1 %	від 0,1 до 0,05 %	від 0,05 до 0,01 %	менше ніж 0,01 %	не критично	$РК_{10}$ =
8.	Заподіяння збитків місцевим бюджетам (зниження прибутків бюджету у відсотках прогнозованого річного прибутку бюджету)	більше ніж 0,1 %	від 0,1 до 0,05 %	від 0,05 до 0,01 %	менше ніж 0,01 %	не критично	$РК_{11}$ =
IV. Взаємозв'язок між об'єктами критичної інфраструктури							
9.	Негативний вплив на безперервне та стійке функціонування іншого об'єкта інфраструктури, що забезпечує надання таких найосновніших послуг	матиме негативний вплив (якщо так, вкажіть який)				не критично	$РК_{12}$ =
10.	Негативний вплив на безперервне та стійке функціонування іншого об'єкта інфраструктури, що надає інші основні послуги	матиме негативний вплив (якщо так, вкажіть який)				не критично	$РК_{13}$ =

Негативний вплив		Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бали)	Рівень негативного впливу: незначні наслідки (1 бал)	Рівень негативного впливу: надто малий (0 балів)	Оцінка РКі
V. Значущість об'єкта критичної інфраструктури для забезпечення національної безпеки та обороноздатності країни							
11.	Припинення або порушення (невиконання встановлених показників) функціонування пунктів управління (ситуаційного центру), що оцінюється в рівні (значущості) пункту управління або ситуаційного центру	припинення або порушення функціонування пунктів управління Верховного Головнокомандувача Збройних Сил, Головнокомандувача Збройних Сил, Начальника Генерального штабу Збройних Сил або ситуаційного центру Офісу Президента України, Кабінету Міністрів України, Ради національної безпеки та оборони України	припинення або порушення функціонування пунктів управління або ситуаційного центру центральних органів виконавчої влади, інших державних органів, органів державного управління, юрисдикція яких поширюється на всю територію України, пунктів управління Сухопутних військ, Повітряних Сил, Військово-Морських Сил, десантно-штурмових військ, сил спеціальних операцій, Національної гвардії, Держприкордон-служби	припинення або порушення функціонування обласної державної адміністрації, ситуаційних центрів	припинення або порушення функціонування територіальних органів центральних органів виконавчої влади	не критично	$РК_{14}$ =
12.	Припинення або порушення виробництва товарів, виконання робіт та надання послуг	*Зниження обсягів продукції (робіт, послуг) в заданий період часу (у відсотках)*					
		більше ніж 15 %	від 10 до 15 %	від 5 до 10 %	менше ніж 5 %	не критично	$РК_{15}$ =
		Збільшення часу виготовлення продукції (робіт, послуг) із заданим обсягом (відсотків встановленого часу на виготовлення продукції)					

Негативний вплив	Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бали)	Рівень негативного впливу: незначні наслідки (1 бал)	Рівень негативного впливу: надто малий (0 балів)	Оцінка РКі
оборонного призначення, які є предметом оборонних закупівель, для забезпечення потреб сектору безпеки і оборони, а також інших товарів, робіт і послуг для гарантованого забезпечення потреб безпеки і оборони	більше ніж 40 %	від 10 до 40 %	від 5 до 10 %	менше ніж 5 %	не критично	$РК_{16}$ =
Усього						

{Додаток 2 із змінами, внесеними згідно з Постановою КМ № 48 від 16.01.2024}

Для нотаток

Навчальне видання

Березняк Василь Сергійович
Бурлака Владислав Васильович
Людвік Валентин Дмитрович
Сидорова Ельвіра Олександрівна
Титаренко Олексій Олексійович
Ткач Юлія Олегівна

КВАЛІФІКАЦІЯ ОКРЕМИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ПРОТИ КРИТИЧНО ВАЖЛИВИХ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ (ст. ст. 259, 360 КК УКРАЇНИ)

Методичні рекомендації

Редактор, оригінал-макет –
А. В. Самотуга

Редактор *О. М. Врублевська*

Підп. до друку 26.07.2024. Формат 60х84/16. Друк – цифровий. Тираж – 35 прим.
Гарнітура – Times New Roman. Ум.-друк. арк. 7,67. Обл.-вид. арк. 8,25. Зам. № 05/24-мр

Надруковано у Дніпровському державному університеті внутрішніх справ
49005, м. Дніпро, просп. Науки, 26, sed@dduvs.edu.ua
Свідоцтво про внесення до державного реєстру ДК № 8112 від 13.06.2024