УДК 342.9
DOI https://doi.org/10.17721/2227-796X.2022.3.01

ЗАХИСТ НАЦІОНАЛЬНОЇ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ: АКТУАЛЬНІ ПРОБЛЕМИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Мета. *Переваги сучасного цифрового світу та розвиток інформаційних технологій зумовили появу нових загроз національній безпеці в інформаційній сфері. Дедалі частіше об'єктами кібератак, кількість та потужність яких постійно зростає, стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій. Тому метою дослідження є пошук шляхів вирішення актуальних проблем захисту національної критичної інформаційної інфраструктури.*

Методи. *Для виконання дослідження були використані різні матеріали і застосовані сукупність загальнонаукових та спеціально-юридичних наукових методів: діалектичний метод, метод системного і контент-аналізу, метод індукції та дедукції, формально-юридичний метод та інші. Ці методи були обрані з урахуванням обраної мети та завдань дослідження.*

Результати. *У статті висвітлено актуальний стан правового регулювання захисту критичної інформаційної інфраструктури України. Запропоновано орієнтовний перелік об'єктів вітчизняної критичної інформаційної інфраструктури, які потребують захисту, для використання в наукових дослідженнях і практиці.*

Зазначено актуальні загрози безпеці критичної інформаційної інфраструктури, визначені у документах стратегічного рівня та додатково уточнені за результатами аналізу матеріалів практики протидії таким загрозам. Такі загрози набувають принципово нового значення в умовах ведення РФ гібридної війни проти України та мають тенденції до посилення їх негативного впливу на стан національної безпеки в різних її сферах.

Безпека та захищеність об'єктів критичної інформаційної інфраструктури від таких загроз визначені в Україні на концептуальному рівні одними із базових елементів національної системи стійкості. Окреслено сучасні проблемні аспекти та потреби захисту об'єктів критичної інформаційної інфраструктури, запропоновані шляхи їх вирішення з урахуванням українського та світового досвіду, у т. ч. законодавчі, організаційні, технічні, режимні, розвідувальні, контррозвідувальні, оперативно-розшукові.

Висновки. *Для України характерними є недоліки правового регулювання функціонування та захисту національної критичної інформаційної інфраструктури, недосконалість державної політики в сфері її захисту в умовах високого ризику вчинення диверсій і терористичних та кібератак на її об'єкти. Тому для організації ефективного захисту ОКІІ України необхідно завершити процес формування законодавчого підґрунтя цієї діяльності, сформувати національну систему захисту таких об'єктів, запровадити єдину методологію забезпечення їх стабільного функціонування. Також доцільно забезпечити упровадження міжнародних стандартів діяльності, налагодження державно-приватного партнерства та розвиток міжнародної співпраці у вказаній сфері.*

Ключові слова: критична інформаційна інфраструктура, захист, об'єкти, потреби, проблеми, вирішення.

Дмитро Мельник,
кандидат юридичних наук, доцент, провідний науковий співробітник Міжвідомчого науково-дослідного центру при Раді національної безпеки і оборони України
orcid.org/0000-0002-1497-950X
d-melnik@ukr.net

1. Вступ

Акції кібернетичного впливу в сучасних умовах стали невід'ємною складовою гібридної агресії РФ проти України. Наша країна стала полігоном для хакерських експериментів спецслужб РФ, численних диверсій і терактів проти об'єктів критичної інфраструктури. Шкідливі вірусні програми ("Black Energy", "WannaCry", "Petya", "Not Petya", "Locky", "Bad Rabbit" тощо) спершу були апробовані в Україні, а потім використовувалися проти критичної інфраструктури країн Заходу (Грицак, 2018; Черняускас, 2016).

Україна протягом 2014–2021 років зазнала безпрецедентної кількості кібератак на інформаційні ресурси об'єктів критичної інфраструктури (далі – ОКІ) – підприємств життєзабезпечення, енергетичної, транспортної сфери, державних фінансових установ, органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій тощо. Безпосереднього шкідливого впливу зазнали інформаційні системи та мережі на таких об'єктах.

Метою дослідження є пошук шляхів вирішення актуальних проблем захисту національної критичної інформаційної інфраструктури.

Методологія. Дослідження проблемних аспектів та потреб захисту об'єктів критичної інформаційної інфраструктури (далі – ОКІІ) України було послідовно реалізовано у декілька етапів. Спершу було проаналізовано стан нормативно-правового регулювання захисту об'єктів національної критичної інформаційної інфраструктури. Надалі визначено наявні загрози та проблеми безпечного функціонування національної критичної інформаційної інфраструктури. Наприкінці роботи зроблені висновки і надані рекомендації з покращення захисту критичної інформаційної інфраструктури.

Для виконання дослідження були використані різні матеріали і застосовані низка методів. Ці методи були обрані з урахуванням обраної мети та завдань дослідження. Зокрема, у роботі автор використав сукупність загальнонаукових та спеціально-юридичних наукових методів: діалектичний метод, метод системного і контент-аналізу, метод індукції та дедукції, формально-юридичний метод та інші.

2. Основний текст

Загрози безпеці критичної інфраструктури. Триваючі процеси глобалізації та стрімкий розвиток інформаційних технологій зумовили появу нових загроз національній критичній інфраструктурі, насамперед кібернетичних та терористичних.

Поряд з традиційними способами вчинення терористичних актів на об'єктах критичної інфраструктури (вибухи, підпали інші пошкодження), терористами широко застосовуються новітні інформаційно-комунікаційні технології для порушення штатних режимів роботи автоматизованих систем управління технологічними процесами. Дедалі більшого розповсюдження у кіберпросторі набуває політично вмотивована діяльність у формі кібератак на державні та корпоративні інформаційні ресурси.

Зростає і технічний рівень реалізації кіберзагроз, постійно вдосконалюються та розробляються нові інструменти і механізми кібератак. Набуває глобального масштабу використання кіберпростору терористичними організаціями. Пріоритетними цілями кібертероризму залишаються об'єкти критичної інфраструктури – атомної енергетики, електро- та водопостачання, сфери електронних комунікацій, фінансової та банківської сфери, авіа- та залізничного транспорту, сховищ стратегічних видів сировини, хімічні й біологічні об'єкти тощо.

Необхідність захисту ОКІІ в сучасних умовах зумовлюють низка серйозних загроз національній безпеці, перелік яких був конкретизований у Стратегії національної безпеки України, затвердженій Указом Президента України від 14.09.2020 № 392/2020.

Серед них: сучасна модель глобалізації, яка уможливила поширення міжнародного тероризму, релігійного та ідеологічного фундаменталізму й екстремізму; продовження РФ гібридної війни проти України шляхом системного застосування воєнних, політичних, економічних, інформаційно-психологічних і кібернетичних засобів; продовження спецслужбами іноземних держав, насамперед РФ, розвідувально-підривної діяльності проти України; посилення загроз для критичної інфраструктури, пов'язаних з погіршенням її технічного стану, відсутністю інвестицій в її оновлення та розвиток, несанкціонованим втручанням у її функціонування, триваючими бойовими діями, тимчасовою окупацією частини території України; використання ресурсів ОКІ для фінансування тероризму, сепаратизму та розповсюдження зброї масового знищення тощо.

Вказаний перелік загроз національній безпеці уточнюється і доповнюється положеннями Стратегії кібербезпеки України, затвердженої Указом Президента України від 26.08.2021 № 447/2021: гібридна агресія РФ проти України у кіберпросторі; кібератаки РФ, спрямовані на інформаційно-комунікаційні системи державних органів України та інші ОКІІ з метою виведення їх з ладу, отримання прихованого доступу і контролю; використання кіберпростору

для вчинення актів кібертероризму, надання фінансової та іншої підтримки терористичної діяльності; кіберзлочинність, що завдає шкоди інформаційним ресурсам та призводить до значних матеріальних втрат; використання кіберпростору для вчинення злочинів, пов'язаних із незаконним поводженням із засобами ураження та іншими предметами і речовинами, небезпечними для життя і здоров'я людей; викрадення чутливої інформації у політичних, економічних або військових цілях; розвідувально-підривна діяльність у кіберпросторі шляхом вчинення тривалих, складних і прихованих кібератак, зорганізованих іншими державами.

Зазначені загрози набувають принципово нового значення в умовах ведення РФ гібридної війни проти України та мають тенденції до посилення їх негативного впливу на стан національної безпеки в різних її сферах.

Також на стан безпеки ОКІ та їх інформаційних ресурсів впливають: недосконаліть національної системи захисту критичної інфраструктури, відсутність єдиного державного органу, що здійснює координацію дій у цій сфері; нечіткість завдань, повноважень та відповідальності суб'єктів захисту критичної інфраструктури; відсутність затвердженого переліку, а також порядку паспортизації і категоризації таких об'єктів та єдиної методології оцінки загроз критичній інфраструктурі тощо.

Такий стан справ створює перешкоди для ефективного виконання першочергових безпекових завдань уповноваженими суб'єктами, не дозволяє організувати ефективний захист ОКІІ, що суттєво підвищує небезпечність відповідних загроз національній безпеці України.

Об'єкти критичної інформаційної інфраструктури. Віднесення об'єктів до ОКІ та формування Реєстру об'єктів критичної інфраструктури здійснюються відповідно до приписів ст. 8 Закону України «Про критичну інфраструктуру» у порядку, встановленому КМ України. Відповідно до ч. 2 ст. 6 Закону України «Про основні засади забезпечення кібербезпеки України» критерії та порядок віднесення до ОКІІ, перелік таких об'єктів, загальні вимоги щодо їх кіберзахисту затверджуються Кабміном та Нацбанком України (у банківській системі).

З урахуванням можливих негативних наслідків, визначених Порядком формування переліку об'єктів критичної інформаційної інфраструктури (Постанова КМУ № 943, 2020), до числа ОКІІ України доцільно віднести інформаційні ресурси (системи електронних комунікацій, бази даних тощо) ***органів державної влади і управління*** (Офіс Президента, РНБО України та її робочий орган Національний координаційний центр кібербезпеки, КМ України, НКРЗ, Нацбанк, ДССЗЗІ України, Національний центр оперативно-технічного управління мережами телекомунікацій України тощо), ***сил безпеки і оборони*** (СБУ, МО України, НПУ, розвідувальні органи), а також підприємства, установи та організації незалежно від форми власності, які є ***власниками (розпорядниками) або операторами об'єктів*** критичної

інформаційної інфраструктури та/або ***провадять діяльність*** у сфері захисту даних, електронних комунікацій і забезпечують їх функціонування, а також системи управління технологічними процесами на ОКІ (Мельник, 2019).

Значення критичної інформаційної інфраструктури як стратегічного ресурсу все більше зростає, що вимагає постійної уваги й належної охорони. Відповідно до приписів ст. 4 Закону ОКІІ є об'єктами кібербезпеки та кіберзахисту. На ОКІ забезпечується захист інформаційно-комунікаційних систем від кібератак, а також проводиться незалежний аудит інформаційної безпеки, вимоги і порядок проведення якого встановлюються нормативно-правовими актами, розробленими на основі міжнародних стандартів, стандартів ЄС і НАТО та затверджених КМ України. Пріоритетному захисту від кібератак підлягають об'єкти, включені до Переліку об'єктів критичної інформаційної інфраструктури (Постанова КМУ № 943, 2020).

Стан захисту об'єктів критичної інфраструктури. З огляду на існування вказаних загроз, перші кроки з удосконалення захисту критичної інфраструктури України були зроблені ще на виконання низки рішень РНБО України, оголошених у 2016–2017 роках. Це переважно вжиті вітчизняними правоохоронними органами заходи щодо забезпечення безпеки, удосконалення захисту критичної інфраструктури України, нейтралізації спроб ускладнити функціонування ОКІ, унеможливлення спроб порушення громадського порядку на її об'єктах (Лапаєв Ю., Голуб А., 2017).

Також вперше за часів незалежності прийняті закони України «Про основні засади забезпечення кібербезпеки України», «Про критичну інфраструктуру», Концепція забезпечення національної системи стійкості (Указ Президента України, 2021), Концепція створення державної системи захисту критичної інфраструктури (розпорядження КМ України, 2017) та Порядок формування переліку об'єктів критичної інформаційної інфраструктури (Постанова КМ України, 2020), оновлена Стратегія кібербезпеки України прискорили процеси формування національної системи кібербезпеки як сукупності суб'єктів її забезпечення та взаємопов'язаних заходів захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури (ч. 1 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України»).

Закон України «Про основні засади забезпечення кібербезпеки України» (ст. 5) визначає широкий перелік суб'єктів забезпечення кібербезпеки – Президент, Кабінет Міністрів, РНБО України, що через свій робочий орган Національний координаційний центр кібербезпеки[1] здійснює координацію та контроль за діяльністю інших суб'єктів, а також низку державних і недержавних суб'єктів, які безпосередньо здійснюють забезпечення

[1] Положення про Національний координаційний центр кібербезпеки, затверджене Указом Президента України від 07.06.2016 № 242/2016. http://zakon2.rada.gov.ua/laws/show/242/2016

кібербезпеки. Відповідно до ст. 8 Закону та Стратегії кібербезпеки України, основу національної системи кібербезпеки становлять ДССЗЗІ, СБУ, НПУ, Міноборони та Генштаб ЗСУ, Нацбанк України, розвідувальні органи, на які покладені відповідні завдання.

Водночас вжиті заходи ще не набули системного характеру і не забезпечили комплексної протидії загрозам, їх нейтралізації й усунення, про що свідчать численні кібератаки на ОКІ, які мали місце упродовж останніх кількох років, та їх наслідки.

Прояви кібератак на ОКІ. Протягом останніх кількох років інформаційні системи та ресурси ОКІ України постійно зазнають кібератак з боку підконтрольних спецслужбам РФ хакерських угруповань та окремих осіб (Вітюк, 2021). Найбільшу небезпеку несли кібератаки на автоматизовані системи дистанційного управління енергетичної і транспортної інфраструктури України (Міненерговугілля, 2017; Укренерго, 2017).

Перша зареєстрована успішна кібератака на енергетичну систему України з виведенням її із ладу сталася ще у грудні 2015 року, коли російським хакерам із використанням троянської програми "BlackEnergy" вдалося атакувати комп'ютерні системи управління низки енергопостачальних компаній: «Київобленерго», «Прикарпаття-обленерго» та «Чернівціобленерго». Найбільше від кібератаки постраждали споживачі «Прикарпаття-обленерго», оскільки було вимкнено близько 30 підстанцій, біля 230 тисяч мешканців залишались без світла протягом 1–4 годин (Міненерговугілля, 2017).

Наступна подібна кібератака сталась вночі з 16 на 17 грудня 2016 року: на підстанції «Північна» стався збій в автоматиці управління. На понад одну годину була виведена з ладу підстанція «Північна» енергокомпанії «Укренерго», без струму залишились споживачі північної частини правого берега м. Києва та прилеглих районів області (Міненерговугілля, 2017). Також у грудні 2016 року жертвами кібернападів з використанням модифікації вірусу "BlackEnergy" стали НБУ та низка державних банків разом з Мінфіном, Держказначейством та Пенсійним фондом України.

Упродовж травня – липня 2017 року комп'ютерні системи низки державних фінустанов та багатьох комерційних структур в Україні зазнали масованої атаки вірусів "WannaCry", "Locky", "Bad Rabbit" та мережевого черв'яка "Petya", розробники яких вимагали значну суму грошей за відновлення доступу до інформації (Лапаєв Ю., Голуб А., 2017).

У жовтні 2017 року комп'ютерні мережі «Київського метрополітену» та аеропорту «Одеса», сайт держзакупівель "ProZorro", а також інформаційні ресурси ДФС України та низки вітчизняних підприємств були атаковані з використанням вірусів "Locky" та "Bad Rabbit" (Лапаєв Ю., Голуб А., 2017).

Вже у січні 2018 року хакери зламали сервер Головного територіального управління юстиції в Одеській області, а у квітні – сайт Міненерговуглепрому України та держпідприємства «Антонов».

У квітні – травні 2019 року правоохоронцями фіксувалися кібератаки з РФ на сервер ЦВК України. У листопаді 2019 року командою "CERT-UA" були заблоковані 11 DDoS-атак на веб-ресурси Офісу Президента України.

На початку травня 2020 року командою "CERT-UA" були заблоковані 9 DDoS-атак на веб-ресурси Офісу Президента України. У серпні 2020 року НКЦК при РНБО України повідомив про підготовку хакерським угрупованням "Armageddon" кібератаки на інформресурси органів влади та ОКІІ напередодні Дня незалежності України. У вересні 2020 року хакери зламали сайт НПУ.

У 2021 році спрямування хакерських угрупувань до ІТС держустанов залишалися сталими у зовнішньополітичній, економічній сферах та секторі безпеки і оборони. Найбільшу небезпеку несли кібератаки на автоматичні системи дистанційного управління енергетичної і транспортної інфраструктури України.

Так у листопаді 2021 року СБУ викрила хакерське угруповання "Armageddon", учасники якого з 2014 року здійснили понад 5 тисяч кібератак на інформаційні ресурси державних органів України. Вони використовували власні вірусні програми і намагався «заразити» понад 1,5 тисячі урядових комп'ютерних систем. Основними цілями зловмисників були: встановлення контролю над об'єктами критичної інфраструктури (електростанції, системи тепло- та водопостачання); викрадення та збір розвідувальних даних, у т. ч. інформації з обмеженим доступом; проведення акцій інформаційно-психологічного впливу; блокування інформаційних систем (Вітюк І., 2021).

У поточному році вищевказані прояви кібертероризму продовжили мати місце та ще більше актуалізувалися з початком повномасштабної військової агресії РФ проти України.

15.02.2022 лютого хакери здійснили потужну DDOS-атаку на веб-сайти органів державної влади (у т. ч. Міноборони України, ЗСУ), банківських установ («Ощадбанк», «ПриватБанк») та портал «Дія». Експерти з цифрової трансформації визначили дестабілізацію та сіяння хаосу в Україні як мету вказаної атаки, яку було здійснено з різних країн (Демедюк С., 2022).

Анонімність та віддаленість доступу кібератак сприяє їх широкому застосуванню проти України. Технічний рівень реалізації кібератак на ОКІ постійно зростає, вдосконалюються та розробляються нові інструменти і механізми їх вчинення. Набуває глобального масштабу використання кіберпростору терористичними організаціями. Міжнародні хакерські угруповання все частіше залучаються іноземними спецслужбами для реалізації акцій кібервпливу[2].

Заходи з покращення захисту критичної інформаційної інфраструктури. Поширення кіберзагроз на усі сфери життєдіяльності, пов'язані з функціонуванням ОКІ, та вдосконалення інструментарію їх реалізації

[2] Стратегія кібербезпеки України, затверджена Указом Президента України від 26.08.2021 № 447/2021. URL: https://www.rnbo.gov.ua/ua/Ukazy/4974.html

зумовлює необхідність зміни стратегії і тактики протидії в умовах триваючої гібридної війни РФ проти України. Потребують перегляду засади забезпечення безпеки критичної інформаційної інфраструктури України.

Безпека та захищеність ОКІ визначена в Україні одним із базових елементів національної системи стійкості, стабільне функціонування яких необхідно забезпечувати, у т. ч.: кібербезпека; захищеність та безперебійне функціонування інформаційних та комунікаційних послуг; безперебійне енерго-, водо-, теплопостачання, постачання продовольства; стійке функціонування транспортних систем (Концепція забезпечення національної системи стійкості, 2021).

Тому для покращення захисту критичної інформаційної інфраструктури вважається за доцільне вжити заходів (Мельник Д., 2019; Мельник Д., 2018):

1) **законодавчих** – унормувати поняття кібертероризму (комп'ютерного тероризму) у ст. 1 Закону України «Про боротьбу з тероризмом»; доповнити Розділ XVI КК України нормою про кримінальну відповідальність за комп'ютерний тероризм, яка б дозволила розмежувати поняття комп'ютерного тероризму та комп'ютерної злочинності; прийняття законів України «Про протидію екстремістській діяльності», «Про перехоплення електронних комунікацій»; розробити і прийняти нормативно-правові акти щодо визначення правових і організаційних засад впровадження та функціонування національної системи стійкості, у т. ч. Стратегії захисту критичної інфраструктури України; вдосконалити нормативно-правове регулювання порядку залучення правоохоронних органів до роботи з попередження, виявлення і припинення актів кібертероризму; посилити кримінальну відповідальності за незаконне втручання в роботу об'єктів критичної інформаційної інфраструктури;

2) **організаційних** – створити ефективну *загальнодержавну систему захисту критичної інформаційної інфраструктури України*, *координації та управління силами і засобами забезпечення її безпеки*, у т. ч.: створити національну систему управління кіберінцидентами, упровадити стандартні операційні процедури для реагування на них для оцінки критичності подій та пріоритетності реагування; розробити Національний план реагування на надзвичайні (кризові) ситуації на ОКІ; упровадити ризик-орієнтований підхід щодо забезпечення кібербезпеки ОКІ, розроблити методики ідентифікації та оцінки кіберризиків для критичної інфраструктури держави; створити державний реєстр ОКІ; запровадити на постійній основі оцінки стану захищеності ОКІ та державних інформаційних ресурсів на вразливість; упровадити систему обов'язкового аудиту інформаційної безпеки на ОКІ, визначити механізми та базові методики проведення аудитів; розвивати та вдосконалювати систему технічного і криптографічного захисту інформації; розвивати мережу команд реагування на комп'ютерні надзвичайні події; поглиблювати міжнародну співпрацю щодо забезпечення стійкості критичної інфраструктури;

3) **технічних** – встановити обов'язкові вимоги (стандарти) інформаційної безпеки ОКІІ з урахуванням міжнародних стандартів та специфіки галузі, до якої належать такі об'єкти; упроваджувати нові алгоритми підвищення рівня кіберстійкості комунікаційних та технологічних систем ОКІ; створювати систему сертифікації продукції, необхідної для функціонування та кіберзахисту інформаційно-комунікаційних систем ОКІ; забезпечувати розвиток організаційно-технічної моделі кіберзахисту, систем технічного і криптографічного захисту інформації, впроваджувати вітчизняні рішення щодо таких видів захисту інформації; визнати пріоритетність використання засобів таких видів захисту інформації вітчизняного виробництва для кіберзахисту державних інформаційних ресурсів та ОКІІ;

4) **режимних, розвідувальних, контррозвідувальних та оперативно-розшукових**, спрямованих на зниження рівня вразливості ОКІІ до кіберзагроз воєнного, кримінального, терористичного та іншого характеру, у т. ч.: створити загальнодержавну систему виявлення кібератак, протидії кібертероризму і кібершпигунству щодо таких об'єктів; розвивати систему контррозвідувального забезпечення кібербезпеки; посилити моніторинг контенту мережі Інтернет та упровадити у практику технологічні рішення, що забезпечують доступ до циркулюючої в ній інформації; забезпечити постійне здійснення заходів з виявлення, попередження і припинення розвідувально-підривної діяльності іноземних держав, актів кібершпигунства та кібертероризму, усунення їх причин і умов; удосконалювати аналітичне і криміналістичне забезпечення контррозвідувального захисту кібербезпеки держави шляхом упровадження інноваційних методик обробки та оцінки цифрових даних, формування електронних доказів; посилювати спроможності державних органів у проведенні негласних перевірок стану готовності ОКІ до можливих кібератак та кіберінцидентів для мінімізації кіберзагроз.

3. Висновки

Таким чином, для України характерними є недоліки правового регулювання функціонування та захисту національної критичної інформаційної інфраструктури, недосконалість державної політики в сфері її захисту в умовах високого ризику вчинення диверсій і терористичних та кібератак на її об'єкти. Тому для організації ефективного захисту ОКІІ України необхідно завершити формування законодавчого підґрунтя цієї діяльності, сформувати загальнодержавну систему захисту таких об'єктів, запровадити єдину методологію забезпечення їх стабільного функціонування. Також доцільно забезпечити упровадження міжнародних стандартів діяльності, налагодження державно-приватного партнерства та розвиток міжнародної співпраці.

Список використаних джерел:

1. Грицак В. Україна стала полігоном для хакерських експериментів спецслужб РФ. Інтерв'ю Голови СБУ інформагентству «Укрінфром». 01.02.2018. URL: http://ukrinform.ua/rubric-politics/2144501-vasil-gricak-golova-sluzbi-bezpeki-ukraini.htm (дата звернення: 10.03.2018).

2. Черняускас Р. У Литві на урядових комп'ютерах виявили російське шпигунське програмне забезпечення. 22.12.2016. URL: http://www.rbc.ua (дата звернення: 10.03.2018).

3. Порядок формування переліку об'єктів критичної інформаційної інфраструктури, затверджений Постановою КМ України від 09.10.2020 № 943. URL: http://zakon2.rada.gov.ua/laws/show/943-2020-п (дата звернення: 12.03.2022).

4. Мельник Д. Національна критична інформаційна інфраструктура України: сучасні потреби захисту її об'єктів. *Збірник наукових праць НА СБУ*. Київ, 2019, № 70. С. 111–119.

5. Лапаєв Ю., Голуб А. Ще один фронт. Як Україна відповідає на виклики, що постали у віртуальному просторі. 19.01.2017. URL: http://tyzhden.ua/publication/183407 (дата звернення: 10.03.2018).

6. Концепція забезпечення національної системи стійкості, затверджена Указом Президента України від 27.09.2021 № 479/2021. URL: https://www.rnbo.gov.ua/ua/Ukazy/5017.html?PRINT (дата звернення: 12.03.2022).

7. Концепція створення державної системи захисту критичної інфраструктури, схвалена розпорядженням КМ України від 06.12.2017 № 1009-р. URL: http://zakon3.rada.gov.ua/laws/show/1009-2017-р (дата звернення: 10.03.2018).

8. Вітюк І. В Україні викрили хакерів ФСБ, які здійснили понад 5 тисяч кібератак на держоргани. 04.11.2021. URL: https://ord-ua.com/2021/11/04/v-ukraini-vikrili-hakeriv-fsb-jaki-zdijsnili-ponad-5-tisjach-kiberatak-na-derzhorgani/ (дата звернення: 05.12.2021).

9. Міненерговугілля оприлюднило звіт про російську кібератаку на обленерго. URL: http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245086886&cat_id=35109 (дата звернення: 10.03.2018).

10. В Укренерго пояснили масштабний збій в енергосистемі під Києвом кібератаками. URL: http://economics.unian.ua/energetics/1689781-v-ukrenergo-poyasnili-masshtabniyzbiy-v-energosistemi-pid-kievom-kiber-atakami.html (дата звернення: 10.03.2018).

11. Демедюк С. Державна система кіберзахисту спрацювала на «відмінно», реагуючи на останню кібератаку, яка була здійснена стосовно державних вебресурсів та банківської системи. URL: https://www.rnbo.gov.ua/ua/Diialnist/5263.html (дата звернення: 12.03.2022).

12. Мельник Д. Щодо актуальних потреб захисту національної критичної інформаційної інфраструктури України. *Актуальні проблеми управління інформаційною безпекою держави :* зб. тез наук. доп. наук.-практ. конф. (Київ, 30.03.2018) [Електронне видання]. Київ : Нац. акад. СБУ, 2018. – С. 112–115 (дата звернення: 05.12.2021).

References:

1. Hrytsak, V. (2018) Ukraina stala polihonom dlia khakerskykh eksperymentiv spetssluzhb RF [Ukraine became a ground for the hacker experiments of the special services of Russian Federation]. Interv'iu Holovy SBU informahentstvu "Ukrinfrom". URL: http://ukrinform.ua/rubric-politics/2144501-vasil-gricak-golova-sluzbi-bezpeki-ukraini.htm

2. Cherniauskas, R. (2016). U Lytvi na uriadovykh komp'iuterakh vyiavyly rosiiske shpyhunske prohramne zabezpechennia [In Lithuania on governmental computers educed Russian spy software]. URL: http://www.rbc.ua

3. Poriadok formuvannia pereliku ob'iektiv krytychnoi informatsiinoi infrastruktury, zatverdzhenyi Postanovoiu KM Ukrainy vid 09.10.2020 № 943. URL: http://zakon2.rada.gov.ua/laws/show/943-2020-p

4. Melnyk, D. (2019) Natsionalna krytychna informatsiina infrastruktura Ukrainy: suchasni potreby zakhystu yii ob'iektiv [National critical informative infrastructure of Ukraine: modern necessities of defence of it's objects]. *Zbirnyk naukovykh prats NA SBU*, no. 70, pp. 111–119.

5. Lapaiev, Yu., Holub, A. (2017). Shche odyn front. Yak Ukraina vidpovidaie na vyklyky, shcho postaly u virtualnomu prostori [Another front. As Ukraine answers on challenges which appeared in virtual space]. URL: http://tyzhden.ua/publication/183407

6. Kontseptsiia zabezpechennia natsionalnoi systemy stiikosti, zatverdzhena Ukazom Prezydenta Ukrainy vid 27.09.2021 № 479/2021. URL: https://www.rnbo.gov.ua/ua/Ukazy/5017.html?PRINT

7. Kontseptsiia stvorennia derzhavnoi systemy zakhystu krytychnoi infrastruktury, skhvalena rozporiadzhenniam KM Ukrainy vid 06.12.2017 № 1009-r. URL: http://zakon3.rada.gov.ua/laws/show/1009-2017-r

8. Vitiuk, I. (2021). V Ukraini vykryly khakeriv FSB, yaki zdiisnyly ponad 5 tysiach kiberatak na derzhorhany [In Ukraine disrobed the hackers of FSB, which carried out over 5 thousand cyberattacs on state organs]. URL: https://ord-ua.com/2021/11/04/v-ukraini-vikrili-hakeriv-fsb-jaki-zdijsnili-ponad-5-tisjach-kiberatak-na-derzhorgani/

9. Minenerhovuhillia opryliudnylo zvit pro rosiisku kiberataku na oblenerho. URL: http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245086886&cat_id=35109

10. V Ukrenerho poiasnyly masshtabnyi zbii v enerhosystemi pid Kyievom kiberatakamy. URL: http://economics.unian.ua/energetics/1689781-v-ukrenergo-poyasnili-masshtabniyzbiy-v-energosistemi-pid-kievom-kiber-atakami.html

11. Demediuk, S. (2022). Derzhavna systema kiberzakhystu spratsiuvala na "vidminno", reahuiuchy na ostanniu kiberataku, yaka bula zdiisnena stosovno derzhavnykh vebresursiv ta bankivskoi systemy [The state system of cybersecurity worked on "five", reacting on last cyberattac, which was carried out in relation to state web resources and banking system]. URL: https://www.rnbo.gov.ua/ua/Diialnist/5263.html

12. Melnyk, D. (2018). Shchodo aktualnykh potreb zakhystu natsionalnoi krytychnoi informatsiinoi infrastruktury Ukrainy [In relation to the actual necessities of defence of national critical informative infrastructure of Ukraine]. *Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy :* zb. tez nauk. dop. nauk.-prakt. konf. (Kyiv, 30.03.2018) [Elektronne vydannia]. Kyiv : Nats. akad. SBU. – Pp. 112–115.

PROTECTION OF NATIONAL CRITICAL INFORMATION INFRASTRUCTURE: ISSUES OF THE DAY AND SOLUTIONS

Dmytro Melnyk,
Ph.D. in Law, Associate Professor,
Leading Researcher of Interdepartmental Research Center
National Security and Defence Council of Ukraine
orcid.org/0000-0002-1497-950X
d-melnik@ukr.net

Advantages of the modern digital world and development of information technologies stipulated appearance of new threats to national security in an information sphere. All more frequent by the objects of cyberattacs, amount and power of which grows constantly, the information resources of financial institutions, enterprises of transport and power engineering, public organs, which guarantee security, defense, safety in case of disasters. Therefore a research purpose is a search of solutions of issues of the day for protection of national critical information infrastructure.
Methods. *For implementation of research different materials were used and applied aggregate of scientific and specially-legal scientific methods: dialectical method, system's method and the analysis of content, method of induction and deduction, formal law method and others. These methods were select taking into account a select purpose and tasks of research.*
Results. *The actual state of the legal adjusting of protection of critical information infrastructure of Ukraine is reflected In the article. The reference list of objects of domestic critical informative infrastructure, which require defence, is offered, for the use in scientific researches and practice. Actual threats are marked to safety of critical informative infrastructure, certain in the documents of strategic level and additionally specified on results the analysis of the materials of practice of counteraction to such threats. Such threats acquire fundamentally a new value in the conditions of conduct of Russian Federation of hybrid war against Ukraine and have tendencies to strengthening of them negative influence on the state of national security in it's different spheres.*
Safety and security of objects of critical informative infrastructure from such threats are certain in Ukraine at conceptual level one of base elements of the national system of firmness. Modern problem aspects and necessities of defence of objects of critical informative infrastructure are outlined, offered paths of their decision taking into account Ukrainian and world experience, in thereby legislative, organizational, technical, regime, reconnaissance, counterespionage and investigation.
Conclusions. *For Ukraine characteristic are lacks of the legal adjusting of functioning and defence of national critical informative infrastructure, imperfection of public policy in the sphere of her defence in the conditions of high risk of feasance of diversions and terrorist and cyberattacs on her objects. Therefore for organization of effective defence of OCII of Ukraine it is necessary to complete the forming of legislative ground of this activity, form the national system of defence of such objects, enter only methodology of providing of them stable functioning. It is also expedient to provide introduction of international standards of activity, adjusting of state-private partnership and development of international cooperation.*

Key words: critical information infrastructure, defence, objects, necessities, problems, solutions.