Правові аспекти формування системи безпеки об'єктів критично важливої інформаційної інфраструктури в Україні

Legal Aspects of Designing Security System for Critical Information Infrastructure in Ukraine

Сергій Єсімов [1], **Руслан Скриньковський** [2], **Мирослав Ковалів** [1], **Ігор Крет** [3]

Serhii Yesimov, Ruslan Skrynkovskyy, Myroslav Kovaliv, Ihor Kret

[1] *Lviv State University of Internal Affairs*
26 Horodotska Street, Lviv, 79007, Ukraine

[2] *Lviv University of Business and Law*
99 Kulparkivska Street, Lviv, 79021, Ukraine

[3] *Lviv Polytechnic National University*
12 Stepana Bandery Street, Lviv, 79013, Ukraine

DOI: 10.22178/pos.36-2

JEL Classification: K30

Received 20.05.2018
Accepted 20.06.2018
Published online 31.07.2018

Corresponding Author:
Ihor Kret
kret.ihor@ukr.net

Анотація. Поява нових видів злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку робить проблему захисту критично важливої інформаційної інфраструктури актуальною, а розвиток інформаційних технологій і систем та удосконалення комунікаційних технологій переносить ці проблеми з площини технічної у площину юридичну.

Критично важлива інформаційна інфраструктура виступає як сукупність територіально розподілених державних і корпоративних інформаційних систем, мереж зв'язку, засобів комутації та управління інформаційними потоками, організаційних структур, має нормативно-правовий механізм регулювання, що забезпечує їх ефективне функціонування. Особливе місце критично важливої інформаційної інфраструктури зумовлює їх ключову роль в забезпеченні нормального функціонування практично всіх сфер життєдіяльності суспільства і держави – політичної, економічної, соціальної, екологічної, військової та інформаційної.

Зміст функціонування системи забезпечення безпеки критично важливої інформаційної інфраструктури включає формування системи забезпечення безпеки і управління системою забезпечення безпеки. Метою системи забезпечення безпеки об'єктів критично важливої інформаційної інфраструктури є забезпечення належного функціонування відповідних об'єктів, в тому числі, в разі реалізації загроз безпеці. При забезпеченні безпеки об'єктів критично важливої інформаційної інфраструктури повинен досягатися баланс інтересів держави та суспільства і інтересів власників об'єктів.

У статті з позиції методології системного аналізу розглянуто правові аспекти формування системи безпеки об'єктів критично важливої інформаційної інфраструктури. На основі аналізу охарактеризовано зміст функціонування системи забезпечення безпеки критично важливої інформаційної інфраструктури, складові системи забезпечення безпеки, необхідність розробки проекту Закону України «Про об'єкти критично важливої інформаційної інфраструктури» та відомчих нормативних актів щодо адміністративних процедур у сфері інформаційної безпеки.

Ключові слова: інформаційна інфраструктура; інформаційна безпека; кібербезпека; система безпеки; об'єкти критично важливої інформаційної інфраструктури.

Abstract. The emergence of the new types of crimes in the field of using electronic counting machines (computers), computer systems and networks and telecommunication networks makes the problem of protecting critically important information infrastructure relevant, and the development of information technologies and systems and the improvement of communication technologies, transfers these problems from the technical plane to the legal one.

Critical information infrastructure acts as a set of territorially distributed state and corporate information systems, communication networks, switching facilities and information flow management, organizational structures and has a regulatory and legal regulation mechanism that ensures their effective functioning. A special place of critically important information infrastructure determines their key role in ensuring the normal functioning of practically all spheres of life of society and the state - political, economic, social, environmental, military and informational.

The content of the security system operation for a critical information infrastructure includes the formation and management of the security system. The purpose of the security system for objects of critical information infrastructure is to ensure the proper functioning of the relevant facilities, including the cases of real threats to security system. When ensuring the security of objects of critical information infrastructure, the balance of interests of the state and society and the interests of the owners of objects must be achieved.

In the article from the point of methodology of system analysis, the legal aspects of forming the security system of objects of critical information infrastructure are considered. On the basis of the analysis, the content of the security system of critical information infrastructure, the content of the security system, the necessity of elaboration of the draft law of Ukraine "On the objects of critical information infrastructure" and departmental normative acts on administrative procedures in the field of information security have been characterized.

Keywords: information infrastructure; informational security; cyber security; security system; objects of critically important information infrastructure.

ВСТУП

Прагнення України до вступу в Європейський Союз і НАТО ставить завданням наближення нормативно-правового регулювання заходів безпеки до рівня вимог Європейського Союзу та стандартів НАТО. Одним зі зазначених напрямів діяльності є забезпечення кібербезпеки. Закон України від 05 жовтня 2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України» передбачає розробку правового регулювання забезпечення кіберзахисту та інформаційної безпеки критично важливої інформаційної інфраструктури в Україні. Порушення нормального функціонування або виведення з ладу вказаних об'єктів може призвести до тяжких наслідків. У зв'язку з цим актуалізується проблема формування обґрунтованої і оптимальної системи захисту критично важливої інформаційної інфраструктури з метою забезпечення надійного функціонування всіх суспільних і державних інститутів.

Аналіз останніх досліджень і публікацій свідчить про те, що ключові питання інформаційної безпеки з різних аспектів теорії адміністративного і інформаційного права досліджували такі вчені, як І. Арістова, І. Березовська, В. Голубєв, В. Гурковський, О. Дзьобань, Р. Калюжний, В. Конах, Б. Кормич, В. Ліпкан, Ю. Максименко, А. Марущак, В. Цимбалюк, О. Юдін, Р. Юсупов та інші. Проте дослідження та наукові праці містять лише фрагментарні наукові розробки у сфері правового регулювання формування системи безпеки об'єктів критично важливої інформаційної інфраструктури України, що потребує проведення спеціальних додаткових досліджень.

Тому *метою статті* є дослідження правових аспектів формування системи безпеки об'єктів критично важливої інформаційної інфраструктури в Україні.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Закон України від 05 жовтня 2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України» дає можливість розглядати критично важливу інформаційну інфраструктуру як сукупність територіально розподілених державних і корпоративних інформаційних систем, мереж зв'язку, засобів комутації та управління інформаційними потоками, організаційних структур, нормативно-правових механізмів регулювання, що забезпечують їх ефективне функціонування [1].

У контексті євроінтеграції під об'єктом критично важливої інформаційної інфраструктури розглядається сукупність інформаційних ресурсів, засобів і систем обробки інформації, використовуваних відповідно до заданої інформаційної технології, засобів забезпечення функціонування такого об'єкта, приміщень або об'єктів (будівель, споруд, технічних засобів), де вони встановлені, персоналу, який здійснює експлуатацію [2, с. 24].

З погляду на дослідження Л. Щербака, С. Гнатюка, В. Сидоренко та О. Шаховал [3], об'єкти інформаційної інфраструктури є критично важливими, якщо:

- забезпечують функціонування екологічно небезпечних і соціально значущих виробництв технологічних процесів, порушення режиму експлуатації, яких може призвести до надзвичайної ситуації техногенного характеру;

- здійснюють функції інформаційної системи, порушення функціонування якої може призвести до тяжких наслідків для національної безпеки в політичній, економічній, соціальній, інформаційній, екологічній та інших сферах;

- забезпечують надання значного обсягу інформаційних послуг, порушення надання яких може призвести до тяжких наслідків для національної безпеки в політичній, економічній, соціальній, інформаційній, екологічній та інших сферах [3].

Відповідно до Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави об'єкти критично важливої інформаційної інфраструктури розділені на дві групи [4]:

1) системи електронних комунікацій, майнові комплекси, що забезпечують виконання певних інформаційно-комунікаційних функцій, наприклад, оператор послуг Інтернету;

2) системи управління технологічними процесами, які є елементами промислових, енергетичних, банківських та інших техніко-технологічних об'єктів, що зв'язані з об'єктами критичної інфраструктури [4].

Особливе місце критично важливої інформаційної інфраструктури зумовлює їх ключову роль в забезпеченні нормального функціонування практично всіх сфер життєдіяльності суспільства і держави – політичної, економічної, соціальної, екологічної, військової та інформаційної.

Порушення нормальної діяльності критично важливої інформаційної інфраструктури призводить до виникнення тяжких наслідків у вигляді:

- втрати державного управління на тривалий термін (наприклад, в результаті порушення зв'язку між державними органами різного рівня підпорядкування, при здійсненні комп'ютерної атаки на державні інформаційні системи тощо);

- надзвичайних ситуацій техногенного характеру (наприклад, припинення руху поїздів на тривалий період, викид значної кількості небезпечних хімічних речовин і зараження великої території тощо);

- відмови на тривалий період досить великого сегмента банківських платіжних систем (наприклад, збої в роботі платіжних терміналів торгових підприємств, банкоматів і т.д.) тощо.

Зазначені наслідки зумовлюють погіршення соціально-економічної обстановки в країні, дестабілізацію внутрішньодержавної ситуації, що в умовах дії Закону України від 18 січня 2018 р. № 2268-VIII «Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях» є недопустимим [5]. Це призводить до заподіяння шкоди конкретній сфері життєдіяльності суспільства та держави – підриву авторитету державної влади, втрати керованості Збройними Силами держави та ін.

У зв'язку з цим держава виділяє в особливу сферу регулювання питання безпеки критично важливої інформаційної інфраструктури та ставить цілі, які повинні досягатися при

експлуатації таких об'єктів. У галузі безпеки критично важливої інформаційної інфраструктури доцільно виділяти два тісно взаємопов'язаних, але різних за змістом напрями, а саме:

1) формування та забезпечення безпечного функціонування системи критично важливої інформаційної інфраструктури, відповідно до техніко-технологічних правил і вимог;

2) забезпечення безпеки критично важливої інформаційної інфраструктури, тобто здійснення правомірної діяльності працівників об'єктів, служби безпеки у взаємодії з співробітниками уповноважених державних органів, іншими юридичними та фізичними особами, щодо реалізації системи правових, організаційних, інженерно-технічних, програмно-апаратних та спеціальних заходів, спрямованих на охорону та захист критично важливої інформаційної інфраструктури та забезпечення дотримання інтересів держави та суспільства (зокрема, реалізація спеціальних заходів, які не зв'язані з інформаційними технологіями: визначення порядку доступу на територію об'єкта, фізична охорона об'єкта тощо).

Зміст функціонування системи забезпечення безпеки критично важливої інформаційної інфраструктури має включати такі компоненти: 1) формування системи забезпечення безпеки; 2) управління системою забезпечення безпеки.

Формування системи забезпечення безпеки критично важливої інформаційної інфраструктури передбачає послідовну реалізацію організаційних заходів, а саме: визначення складу системи забезпечення безпеки; безпосереднє створення системи, що ґрунтується на сформованих підходах у галузі забезпечення безпеки суб'єктів господарювання.

Як зазначає Т. Ткачук, інформаційна безпека є складним, системним, багаторівневим явищем, на стан якого впливають зовнішні і внутрішні чинники [6, с. 185]. До складу системи забезпечення безпеки об'єктів критично важливої інформаційної інфраструктури повинні входити такі складові, як:

- правова основа, яку складають правові норми, що групуються за рівнями – конституційний рівень – норми Конституції України, що визначають основні положення права власності, забезпечення екологічної та техногенної безпеки, діяльності державних органів щодо забезпечення прав і свобод людини та громадянина;

- базовий рівень – норми спеціального законодавчого акту у сфері забезпечення безпеки об'єктів критично важливої інформаційної інфраструктури, що визначають: правовий статус об'єктів; суб'єктів державного управління в цій галузі і їх функції; систему та зміст заходів забезпечення безпеки, порядок їх застосування тощо;

- функціональний рівень – норми законодавчих актів, постанов Кабінету Міністрів України, приписи нормативно-правових актів уповноважених державних органів і власників об'єктів, що деталізують питання реалізації заходів забезпечення безпеки;

- рівень забезпечення – норми актів законодавства, що безпосередньо не регламентують забезпечення безпеки об'єктів критично важливої інформаційної інфраструктури, але визначають умови реалізації заходів забезпечення безпеки, повноваження державних і інших органів щодо реалізації заходів;

- техніко-технологічний рівень – норми державних технічних стандартів, що регламентують правила будівництва, техніки безпеки, інформаційної безпеки, інші норми технічного регулювання.

До суб'єктів забезпечення безпеки об'єктів критично важливої інформаційної інфраструктури відносяться:

- працівники об'єкта (у тому числі служби безпеки, спеціальні підрозділи з інформаційної безпеки та ін.), які реалізують заходи забезпечення безпеки об'єкта, які передбачені локальними нормативно-правовими актами;

- співробітники уповноважених державних органів (правоохоронних, безпеки, з питань надзвичайних ситуацій тощо), які реалізують заходи забезпечення безпеки об'єкта відповідно до компетенції, визначеної законодавством;

- працівники організацій, які здійснюють проектування, монтаж, наладку та технічне обслуговування засобів і систем охорони;

- інші особи, які в установленому законодавством порядку уповноважені здійснювати охорону і захист (наприклад, адвокати, працівники аудиторських і інших установ та організацій).

Наявність об'єктів критично важливої інформаційної інфраструктури обумовлює розробку певних адміністративних процедур, що здійснюються уповноваженими органами у сфері забезпечення інформаційної безпеки для впорядкування діяльності державних органів і зацікавлених суб'єктів. Адміністративні процедури можуть бути визначенні у Законі України «Про об'єкти критично важливої інформаційної інфраструктури».

З погляду на дослідження О. Бусол «Тенденції нормативно-правового забезпечення інформаційної безпеки США» адміністративні процедури щодо критично важливої інформаційної інфраструктури узагальнено у Наказі президента США «Щодо проекту Стратегії покращення кібербезпеки критично важливих об'єктів інфраструктури (2013 рік)» [7].

При підготовці проекту Закону «Про об'єкти критично важливої інформаційної інфраструктури» доцільно використати положення прийнятих Законів України від 05 липня 1994 р. № 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах», від 18 листопада 2003 р. № 1280-IV «Про телекомунікації», Стратегії національної безпеки України, Стратегії кібербезпеки України та інших нормативно-правових актів.

Проект Закону України «Про об'єкти критично важливої інформаційної інфраструктури» повинен регулювати систему заходів забезпечення безпеки об'єктів критично важливої інформаційної інфраструктури, включати:

- правові заходи – вимоги до локальних нормативних актів у сфері безпеки зазначених об'єктів, у тому числі технічних нормативно-правових актів, дії уповноважених суб'єктів забезпечення безпеки щодо їх реалізації;

- організаційні заходи – дії уповноважених суб'єктів забезпечення безпеки, спрямовані на організацію та підтримку системи забезпечення безпеки об'єктів;

- інженерно-технічні заходи – дії уповноважених суб'єктів забезпечення безпеки, спрямовані на підтримку функціонування об'єктів у проміжок часу в разі виходу з ладу критичних і інших елементів, створення та підтримання систем фізичної охорони об'єктів;

- апаратно-програмні заходи – дії уповноважених суб'єктів забезпечення безпеки, спрямовані на захист інформаційних ресурсів, що обробляються та зберігаються в інформаційних системах або в окремих комплексах програмно-технічних засобів;

- спеціальні заходи – дії уповноважених суб'єктів забезпечення безпеки, спрямовані на попередження, виявлення та локалізацію загроз безпеки об'єктів, здійснення інформаційно-аналітичної діяльності і організацію фізичної охорони працівників об'єкта.

Метою системи забезпечення безпеки об'єктів критично важливої інформаційної інфраструктури є забезпечення належного функціонування відповідних об'єктів, в тому числі, в разі реалізації загроз їх безпеки. При забезпеченні безпеки об'єктів критично важливої інформаційної інфраструктури повинен досягатися баланс інтересів держави та суспільства і інтересів власників об'єктів.

Як зазначає Ю. Лісовська, одним з напрямів превентивних заходів у системі інформаційної безпеки полягає в ефективному, якісному реформуванні законодавства, що стосується інформаційної безпеки [8, с. 105]. Безпосереднє створення системи забезпечення безпеки об'єктів критично важливої інформаційної інфраструктури повинно бути відображено у відомчому нормативному акті та включати таку сукупність заходів, а саме:

- встановлення рівнів забезпечення безпеки, які поділяються на такі види: загальний рівень, на якому заходи забезпечення безпеки об'єктів реалізується працівниками структурних підрозділів, співробітниками уповноважених державних органів, іншими уповноваженими особами; спеціальний рівень, на якому заходи реалізується працівниками служби безпеки об'єкта; аналіз, визначення та моделювання загроз безпеці і інцидентів безпеки; проведення першочергових заходів, основними з яких є розробка: концепції забезпечення інформаційної безпеки об'єкта; положення про службу безпеки об'єкта, положення про підрозділ інформаційної безпеки тощо;

- типові плани: підвищеної готовності об'єкта до діяльності в умовах реалізації загроз; дій персоналу об'єкта при реалізації загроз безпеки та виникненні інцидентів безпеки; забезпечення безпеки в особливих умовах.

Відомчий нормативний акт має стати складовою частиною цілісного пакету концептуальних і нормативно-правових пропозицій у

сфері забезпечення інформаційної безпеки. Основною метою розробки локального нормативного акту є необхідність формування механізму реалізації повноважень державних органів, прав і законних інтересів зацікавлених суб'єктів у сфері експлуатації об'єктів критично важливої інформаційної інфраструктури у межах забезпечення інформаційної безпеки та нормального функціонування життєво важливих елементів інформаційно-телекомунікаційної інфраструктури.

Основними завданнями при цьому є:

- встановлення єдиного підходу до переліку адміністративних процедур і рівнів їх реалізації з урахуванням основних положень законодавства у сфері безпеки об'єктів критично важливої інформаційної інфраструктури;

- формування загального переліку документів і відомостей, що подаються до уповноваженого органу для здійснення адміністративної процедури;

- вироблення механізму реалізації адміністративних процедур з урахуванням вимог законодавства про об'єкти критично важливої інформаційної інфраструктури і технікотехнологічних особливостей інформаційних систем;

- розробка єдиної та скоординованої системи правових, організаційних, інженерно-технічних, програмно-апаратних, спеціальних заходів забезпечення безпеки зазначених об'єктів, що забезпечує безпечне введення в експлуатацію, експлуатацію та виведення з експлуатації відповідних об'єктів;

- визначення органу, уповноваженого на проведення адміністративної процедури контролю і термінів її здійснення.

На сьогодні, зазначають Є. Мануйлов та Ю. Калиновський, захист інформаційного суверенітету країни та забезпечення інформаційної безпеки є справою не тільки державних органів, але й приватних структур, суб'єктів громадянського суспільства [9, с. 18].

Підвідомчість уповноважених суб'єктів у сфері безпеки розподіляється в залежності від завдань, які вони вирішують:

- власники реалізують повноваження виключно щодо об'єктів критично важливої інформаційної інфраструктури, що належать їм (або володіють);

- уповноважені державні органи в галузі безпеки об'єктів критично важливої інформаційної інфраструктури реалізують повноваження за двома напрямами: при здійсненні контролю та нагляду в галузі безпечного функціонування об'єктів; при реалізації функції забезпечення безпеки об'єктів;

- юридичні та фізичні особи при здійсненні допоміжних функцій у сфері забезпечення безпечного функціонування та забезпечення безпеки об'єктів критично важливої інформаційної інфраструктури (наприклад, адвокати, працівники залучених аудиторських організацій або комерційних організацій, що спеціалізуються на наданні послуг з налагодження охоронних систем тощо).

Предметом правового регулювання у межах відомчого нормативного акту є правові та організаційно-управлінські відносини, які пов'язані з формуванням механізму реалізації повноважень державних органів, прав і законних інтересів зацікавлених суб'єктів у сфері експлуатації об'єктів критично важливої інформаційної інфраструктури.

Необхідність розробки Закону України «Про об'єкти критично важливої інформаційної інфраструктури», відомчих нормативно-правових актів щодо визначення та реалізації адміністративних процедур обумовлена:

по-перше, зростанням числа критично важливих об'єктів в системі об'єктів інформаційно-телекомунікаційної інфраструктури;

по-друге, доцільністю розробки механізму реалізацій повноважень державних органів і зацікавлених суб'єктів в даній сфері, що знайшло відображення у Концепції створення державної системи захисту критичної інфраструктури [10];

по-третє, відсутністю нормативно закріплених основ діяльності забезпечення нормального функціонування об'єктів критично важливої інформаційної інфраструктури;

по-четверте, важливістю встановлення загальних підходів до змісту адміністративних процедур, переліком органів, що їх здійснюють, очікуваних результатів реалізації;

по-п'яте, необхідністю реалізації Воєнної доктрини України.

Прийняття зазначених нормативних актів дозволить створити ефективний організаційно-правовий механізм реалізації повнова-

жень державних органів у сфері експлуатації об'єктів критично важливої інформаційної інфраструктури, що забезпечує формування та розвиток системи забезпечення безпеки, спрямований на:

- узгодження єдиних підходів щодо розробки переліку адміністративних процедур і їх змісту;

- визначення компетентних державних органів уповноважених на реалізацію адміністративних процедур у сфері забезпечення інформаційної безпеки;

- адаптацію національних законів і нормативних актів у сфері інформаційної безпеки з метою формування єдиного інформаційного простору та розширення інтеграції в структури Північно-Атлантичного договору, у контексті Закону України «Про Національну безпеку України».

ВИСНОВКИ

Результати проведеного дослідження доводять, що реалізація Стратегії національної безпеки України призвела до прискореної розробки та впровадження у практичну діяльності органів державної влади нормативно-правових актів у сфері інформаційної безпеки. Поява Стратегії кібербезпеки України, постанови Кабінету Міністрів України від 23 серпня 2016 р. № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави», Закону України від 05 жовтня 2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України» свідчить про те, що проблема формування системи забезпечення та безпечного функціонування об'єктів критично важливої інформаційної інфраструктури є важливою і актуальною. У сфері безпеки об'єктів критично важливої інформаційної інфраструктури необхідно виділяти два тісно взаємопов'язаних, але різних за змістом напрями: 1) формування та забезпечення безпечного функціонування системи; 2) забезпечення безпеки. Розробка проекту Закону України «Про об'єкти критично важливої інформаційної інфраструктури», відомчих нормативно-правових актів щодо визначення та реалізації адміністративних процедур направлено на: підтримання стабільного управління державою або адміністративно-територіальною одиницею; підтримання сталого рівня економіки держави або адміністративно-територіальної одиниці; підтримання належного рівня життєдіяльності населення, яке проживає на території держави або адміністративно-територіальної одиниці; створення умов безпечного функціонування інформаційно-телекомунікаційних систем України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ / REFERENCES

1. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [About the basic principles of providing cyber security of Ukraine] (Ukraine), 5 October 2017, No 2163-VIII. Retrieved June 1, 2018, from http://zakon2.rada.gov.ua/laws/show/2163-19 (in Ukrainian)
[Про основні засади забезпечення кібербезпеки України (Україна), 5 жовтня 2017, № 2163-VIII. Актуально на 01.06.2018. URL: http://zakon2.rada.gov.ua/laws/show/2163-19].

2. Smetana, M. (2015). *Zashhita kriticheskoj infrastruktury. Podhody gosudarstv Evropejskogo Sojuza k opredeleniju jelementov kriticheskoj infrastruktury* [Protect critical infrastructure. The approaches of the European Union states to the definition of critical infrastructure elements]. Retrieved from https://fbishheb.vsb.cz/moldavia/files/_KI_Smetana.pdf (in Russian)
[Сметана, М. (2015). *Защита критической инфраструктуры. Подходы государств Европейского Союза к определению элементов критической инфраструктуры*. URL: https://fbiweb.vsb.cz/moldavia/files/_KI_Smetana.pdf].

3. Shcherbak, L., Hnatiuk, S., Sydorenko, V., & Shakhoval, O. (2017). Metod vyznachennia rivnia vazhlyvosti obiektiv krytychnoi informatsiinoi infrastruktury v haluzi tsyvilnoi aviatsii [Method of determination the level of the state critical infrastruc-ture importance in the civil aviation]. *Bezpeka informatsii, 23*(1), 27–38. doi: 10.18372/2225-5036.23.11565 (in Ukrainian)
[Щербак, Л., Гнатюк, С., Сидоренко, В., & Шаховал, О. (2017). Метод визначення рівня

важливості об'єктів критичної інформаційної інфраструктури в галузі цивільної авіації. *Безпека інформації, 23*(1), 27–38. doi: 10.18372/2225-5036.23.11565].

4. Pro zatverdzhennia Poriadku formuvannia pereliku informatsiino-telekomunikatsiinykh system obiektiv krytychnoi infrastruktury derzhavy [On Approval of the Procedure for the Formation of the List of Information and Telecommunication Systems of the State Critical Infrastructure Facilities] (Ukraine), 23 August 2016, No 563. Retrieved June 1, 2018, from http://zakon2.rada.gov.ua/laws/show/563-2016-%D0%BF (in Ukrainian)
[Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави (Україна), 23 серпня 2016, № 563. Актуально на 01.06.2018. URL: http://zakon2.rada.gov.ua/laws/show/563-2016-%D0%BF].

5. Pro osoblyvosti derzhavnoi polityky iz zabezpechennia derzhavnoho suverenitetu Ukrainy na tymchasovo okupovanykh terytoriiakh u Donetskii ta Luhanskii oblastiakh [] (Ukraine), 18 January 2018, No 2268-VIII. Retrieved June 1, 2018, from http://zakon2.rada.gov.ua/laws/show/2268-19 (in Ukrainian)
[Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях (Україна), 18 січня 2018, № 2268-VIII. Актуально на 01.06.2018. URL: http://zakon2.rada.gov.ua/laws/show/2268-19].

6. Tkachuk, T. (2017). Suchasni zahrozy informatsiinii bezpetsi derzhavy: teoretyko-pravovyi analiz [Modern threats to information security of the state: theoretical and legal analysis]. *Pidpryiemnytstvo, hospodarstvo i pravo, 10*, 182–186 (in Ukrainian)
[Ткачук, Т. (2017). Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. *Підприємництво, господарство і право, 10*, 182–186].

7. Busol, O. (2017). Tendentsii normatyvno-pravovoho zabezpechennia informatsiinoi bezpeky SShA [Trends of Regulatory Legal Support of Information Security in the United States]. *Naukovi pratsi Natsionalnoi biblioteky Ukrainy imeni V. I. Vernadskoho, 46*, 92–106 (in Ukrainian)
[Бусол, О. (2017). Тенденції нормативно-правового забезпечення інформаційної безпеки США. *Наукові праці Національної бібліотеки України імені В. І. Вернадського, 46*, 92–106].

8. Lisovska, Yu. P. (2017). Kontseptsiia preventyvnykh zakhodiv u systemi informatsiinoi bezpeky Ukrainy: administratyvno-pravovyi aspekt [Concept of preventive measures in the system of information security of Ukraine: administrative-legal aspec]. *Naukovi pratsi MAUP. Seriia: Yurydychni nauky, 1*, 103–109 (in Ukrainian)
[Лісовська, Ю. П. (2017). Концепція превентивних заходів у системі інформаційної безпеки України: адміністративно-правовий аспект. *Наукові праці МАУП. Серія: Юридичні науки, 1*, 103–109].

9. Manuilov, Ye. M., & Kalynovskyi, Yu. Yu. (2017). Aksiolohichnyi vymir informatsiinoi bezpeky ukrainskoi derzhavy [Axiological dimension of Ukrainian information security]. *Visnyk Natsionalnoho universytetu "Iurydychna akademiia Ukrainy imeni Yaroslava Mudroho". Seriia: Filosofiia, filosofiia prava, politolohiia, sotsiolohiia, 3*(34), 13–30 (in Ukrainian)
[Мануйлов, Є. М., & Калиновський, Ю. Ю. (2017). Аксіологічний вимір інформаційної безпеки української держави. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». Серія: Філософія, філософія права, політологія, соціологія, 3*(34), 13–30].

10. Pro skhvalennia Kontseptsii stvorennia derzhavnoi systemy zakhystu krytychnoi infrastruktury [On Approval of the Concept for the Creation of a State System for the Protection of Critical Infrastructure] (Ukraine), 06 December 2017, No 1009-p. Retrieved June 1, 2018, from http://zakon2.rada.gov.ua/laws/show/1009-2017-%D1%80 (in Ukrainian)
[Про схвалення Концепції створення державної системи захисту критичної інфраструктури (Україна), 06 грудня 2017, № 1009-р. Актуально на 01.06.2018. URL: http://zakon2.rada.gov.ua/laws/show/1009-2017-%D1%80].