Денис Євгенійович ДЕНИЩУК,
науковий співробітник науково-дослідної лабораторії
з проблем досудового розслідування
Харківського національного університету внутрішніх справ;
Маргарита Сергіївна СИРОМЯТНІКОВА,
науковий співробітник науково-дослідної лабораторії
з проблем наукового забезпечення правоохоронної
діяльності та якості підготовки кадрів
Харківського національного університету внутрішніх справ

ОХОРОНА ДЕРЖАВНОЇ ТАЄМНИЦІ В КОНТЕКСТІ НОВИХ ПІДХОДІВ ДО ЗАБЕЗПЕЧЕННЯ НАЛЕЖНОГО РІВНЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Цілеспрямована діяльність держави щодо охорони таємної інформації має доволі тривалу історію. Вивченню її розвитку присвячені дослідження таких вчених як: В. Артемов, Б. Бернадський, О. Ботвінкін, А. Гуза, І. Жевелєва, В. Окіпнюк, В. Сідак, О. Шамсутдінов та інших. Виникнення необхідності в охороні державної таємниці перед усім дослідниками пов'язується із формуванням у світі достатньо стійкого розвідувального інтересу та потребою держав йому протидіяти.

Зараз чинний Закон України 1994 року «Про державну таємницю» так розкриває зміст терміну «охорона державної таємниці» (охорона ДТ): це «комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв» [1, ст. 1].

Підкреслимо, що процитований документ існує близько 28 років. Наразі він є єдиним, серед численних національних підзаконних нормативно-правових актів виданих за часів незалежності України для всебічного врегулювання питань, що стосуються державної таємниці, який посідає місце закону. Названий закон пережив 24 редакції. Проте, наведене нами визначення лише один раз зазнало невеличкого уточнення (у 1999 році, під час першого редагування закону). Отже, є підстави стверджувати, що основний зміст діяльності з охорони ДТ визначено доволі вдало і на теперішній день він залишається незмінним.

Разом із тим, дослідники доходять висновків, що розбудова системи охорони ДТ пройшла низку етапів свого становлення: напрацювання належної нормативно-правової бази, визначення основних учасників (суб'єктів) системи охорони ДТ, побудова їх організаційних структур, налагодження та відпрацювання взаємодії тощо. З цього приводу І. Жевелєва наголошує: «після набуття Україною незалежності тривалий час зберігалася радянська модель захисту інформації з обмеженим доступом, однак після 2014 року активно почала формуватися європейська модель; гостра потреба у появі та подальшому розвитку взаємодії Служби безпеки України із суб'єктами господарювання у сфері захисту інформації з обмеженим доступом з'явилася саме в роки незалежності України з розвитком економічного потенціалу країни, а також усвідомленням того, що забезпечення інформаційної безпеки суб'єктів господарювання є важливою частиною національної безпеки держави» [2, с. 16].

Виходячи з викладеного, логічно припустити, що розвиток системи охорони ДТ ще далеко незавершений. І його перебіг має відповідати вимогам сьогодення та викликам принаймні найближчого майбутнього. Спираючись на це, поставимо собі за мету: визначити вимоги до організації охорони ДТ, що мають відповідати новим підходам до забезпечення національної безпеки.

Говорячи про безпеку зазвичай, перш за все, йдеться про виявлення, прогнозування, протидію та запобігання певним загрозам. Але, що робити в разі коли загрози неминучі, або ресурсів для їх запобігання (чи повного виключення) недостатньо? Наприклад, кібератаки та кіберінциденти відбуваються та будуть продовжуватись завжди (варіює лише їх інтенсивність). При цьому, із розвитком діджиталізації небезпека від них лише зростає. Ще більш загрозливою в такому ракурсі виглядає зміна клімату. Наразі ще невідомі ані прогнозовані наслідки останньої (економічні, соціологічні тощо), ані чи здатне людство взагалі протиставити цій загрозі хоча б щось дієве.

Усвідомивши такий стан справ науковці, практики та посадовці у всьому світі поступово доходять висновків про необхідність мінімізації шкоди від частини вірогідних загроз. Такий підхід призвів до формування концептуально нової ідеї безпеки – виділення критичної інфраструктури та забезпечення її належної безпеки-стійкості.

«Захист критичної інфраструктури як безпековий напрям був започаткований у США ще у період «холодної війни», а на початку нинішнього століття став активно розвиватися у провідних країнах світу як відповідь на різке зростання терористичних загроз» [3, с. 3]. У 2008 році термін «критична інфраструктура» (КІ) знаходить своє закріплення в міжнародному правовому акті виданому ЄС – Директива ЄК 2008/114 від 8 грудня 2008 року «Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту». У нашій державі в 2015 році Національним інститутом стратегічних досліджень видана «Зелена книга з питань захисту критичної інфраструктури в Україні».

До розробки проблематики КІ долучилось багато зарубіжних та вітчизняних науковців. Серед них: та А. Біалас, Д. Бірюков, Д. Бобро, В. Волошин, О. Джафарова, Р. Дженкінс, Д. Дубов, С. Іванюта, Т. Келлі, С. Кондратов, А. Лазарі, В. Майєр, М. Мельник, О. Насвіт, М. Перман, О. Суходоля, А. Фекете, Р. Хантер, П. Хокстад С. Шатрава, С. Якубовський та інші. У 2022 році опублікована змістовна монографія О. Резнікової «Національна стійкість в умовах мінливого безпекового середовища».

Відповідні нормативно-правові напрацювання зроблені також законотворцями України. Так, ще у 2017 році термін «критична інформаційна інфраструктура» було закріплено в Законі України «Про основні засади забезпечення кібербезпеки України». А наприкінці 2021 року був прийнятий Закон України «Про критичну інфраструктуру». Нещодавно (у червні 2022 року) цей закон вступив в дію. Зокрема в ньому йдеться про *створення* Уповноваженого органу у сфері захисту критичної інфраструктури України, який має забезпечувати формування та реалізацію державної політики в сфері захисту КІ. Разом із тим, наприкінці жовтня в означені норми були внесені зміни (№ 2684-IX від 18.10.2022, розпочнуть діяти з грудня). Згідно останніх, Уповноважений орган не створюється, а *визначається* Кабінетом Міністрів України. Крім того, «під час дії воєнного стану, а також протягом 12 місяців після його припинення чи скасування повноваження уповноваженого органу … здійснюються Державною службою спеціального зв'язку та захисту інформації України» [4].

Висновки. На сьогодні поняття «критична інфраструктура» знайоме мабуть кожному громадянину України. Проте, із зрозумілих причин розбудова системи безпеки-стійкості КІ відбувається із певними труднощами. Наразі навіть складно визначити перелік установ, підприємств та організацій, які мають належати до КІ. Тим більше важко спрогнозувати, чи будуть об'єкти КІ у післявоєнний час лише поновлюватись, чи відбудовуватимуться у якісно новому вигляді. В цьому контексті важливо звернути увагу на те, що переважна частина об'єктів майбутньої КІ на сьогодні аж ніяк не режимні.

Отже, в післявоєнний період прогнозовано постане потреба уточнювати зміст окремих відомостей, що становлять державну таємницю в системі забезпечення безпеки-стійкості КІ. В свою чергу, для цього майбутньому Голові Уповноваженого органу в сфері захисту критичної інфраструктури України знадобиться статус державного експерта з

питань таємниць. Крім того, з високою ймовірністю слід очікувати зростання кількості режимно-секретних органів (РСО), які потребуватимуть великої кількості якісно підготовлених співробітників. Розуміючи це, вже зараз варто готуватись до проведення масштабної навчально-кадрової роботи.

Таким чином, напрями розбудови системи охорони ДТ залишаються схожими до тих, які вже спостерігались раніше під час історичного становлення системи забезпечення охорони державної таємниці. А саме: структурно-організаційні, нормативно-правові, та навчально-кадрові. Проте, підводячи підсумок, наголосимо, що забезпечення охорони ДТ на об'єктах системи господарювання КІ дуже вірогідно стане одним з най масштабніших напрямів підтримання інформаційної безпеки вже у досить близькому майбутньому.

Список бібліографічних посилань

1. Про державну таємницю : Закон України від 21.01.1994 р. № 3855-XII (із змінами). Відомості Верховної Ради України (ВВР), 1994, № 16, ст. 93. URL: https://zakon.rada.gov.ua/laws/show/3855-12/ed20220315#top (дата звернення: 19.11.2022).

2. Жевелєва І.С. Генезис діяльності органів державної безпеки щодо захисту інформації з обмеженим доступом в Україні. *Юридичний науковий електронний журнал.* 2021. № 5/2021. С. 12-16.

3. Зелена книга з питань захисту критичної інфраструктури в Україні. Національний інститут стратегічних досліджень. Київ. 2015. 35 с.

4. Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України : Закон України від 18.10.2022 р. № 2684-IX. URL: https://zakon.rada.gov.ua/laws/show/2684-20 (дата звернення: 19.11.2022).

Олена В'ячеславівна ДЖАФАРОВА,
доктор юридичних наук, професор,
професор кафедри поліцейської діяльності
та публічного адміністрування факультету № 3
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0003-4201-0218;
Сергій Олександрович ШАТРАВА,
доктор юридичних наук, професор,
завідувач науково-дослідної лабораторії з проблем досудового розслідування
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-7072-961X

ДЕЯКІ АСПЕКТИ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ПРАВ ЛЮДИНИ В УМОВАХ ВОЄННОГО СТАНУ

Розбудова України як демократичної, правової, соціальної держави, закріплення в Конституції України положення про найвищу соціальну цінність людини, її життя і здоров'я, честі і гідності, недоторканості і безпеки вимагає формування нових підходів до захисту прав людини. Україна проголосила себе правовою державою. А однією з надзвичайно важливих рис правової держави є визнання і дія принципу верховенства права, правового порядку, який ґрунтується на засадах, відповідно до яких ніхто не може бути примушеним робити те, що не передбачено законом. Сутність верховенства права втілена у принципах чесності, справедливості, прозорості та відповідальності. Ці