4. Kummel G., Cottey A., Edmunds T., Forster A. Democratic Control of the Military in Post-Communist Europe. Slavic Review. 2004. 62(1). 145 p.
5. Special Inspector General for Afghanistan Reconstruction (SIGAR). Quarterly Report to the United States Congress. Washington, 2021. 214 p.
6. Wim F. van Eekelen. Democratic Control of Armed Forces: The National And International Parliamentary Dimension. Geneva : DCAF, 2002. 167 p.
7. Cohen A. The Israeli Supreme Court's Political Role in Matters of National Security (February 3, 2014). DOI: http://dx.doi.org/10.2139/ssrn.2390411
8. Про національну безпеку України : Закон України від 21 черв. 2018 р. № 2469-VIII. *Відомості Верховної Ради України.* 2018. № 31. Ст. 241.

Хахановський Валерій Георгійович, *професор кафедри інформаційних технологій навчально-наукового інституту права та психології НАВС, доктор юридичних наук, професор*

ОСНОВНІ СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

Закон України «Про інформацію» (ст. 1) встановлює правила у сфері створення, накопичення, отримання, утримання, застосування, розповсюдження, оборони та захисту інформаційних даних. Згідно з цим законом, захист інформації охоплює комплекс правових, управлінських, організаційних, технічних та інших дій, що спрямовані на забезпечення збереження та неушкодженості інформації, а також належний порядок її отримання [1].

Широке впровадження інформаційних технологій спричинило розповсюдження величезних обсягів інформації у комунікаційних та обчислювальних мережах. У той самий час, помітно зросли можливості для несанкціонованого доступу до інформації через передові технічні пристрої.

Початок розвитку захисту інформації, як спроби приховати інформацію від сторонніх поглядів, можливо віднести до V століття до н.е., коли давньогрецький історик Геродот ввів концепцію тайнопису (криптографії). Сьогодення інформаційної безпеки як науки акумулює багато площин та сфер, ключовими з яких є: «інформаційна безпека держави», що обіймає центральні вектори загальнодержавного захисту інформації. До них належить створення моделей загроз інформаційній безпеці країни та протидія їм (охорона державних та військових таємниць, систем урядового зв'язку, гарантування інформаційної безпеки особи, судочинства, забезпечення інформаційної незалежності та ін.); технічний захист інформації; криптографічний захист інформації. Також існує стеганографічний захист інформації.

Інформаційна безпека у державних органах влади зосереджена на захисті цілісності інформації, яка використовується в їхній діяльності, і має специфічні риси. Передусім, це стосується інформації, яка містить державну таємницю. Окрім того, важливий захист для конфіденційних відомостей у автоматизованих системах, засобах зв'язку та в робочих областях підрозділів. Державні органи влади також повинні бути відповідним чином захищені від дезінформаційних впливів.

Відтак, варто зазначити, що згідно з законодавчими актами України, інформація розглядається як об'єкт права. При кваліфікації правопорушень, де предметом зазіхання виступає інформація (накшталт державної чи комерційної таємниці), допустимо використовувати весь комплекс наявних засобів захисту – не лише цивільного та адміністративного, але й кримінального права.

Основні принципи технічного захисту інформації визначені у «Концепції технічного захисту інформації в Україні». В державних установах розроблено нормативно-правові акти, що визначають порядок організації, нагляду та реалізації робіт, застосування засобів захисту інформації, їх інспектування, атестації, надання ліцензій та дозволів.

Серед загальнодержавних актів щодо технічного захисту інформації можна назвати: ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення; ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Проведення робіт; Тимчасові рекомендації з технічного захисту інформації від витоку по каналах побічних електромагнітних випромінювань та наводок (ТР ТЗІ ПЕМВН–95).

Отже, можна визнати, що нормативно-правова основа з питань гарантування безпеки та захисту інформації в Україні загалом сформована та поступово розвивається. Разом з тим, у питанні безпосереднього забезпечення безпеки та захисту інформації в інтегрованих банках даних державних органів влади України, нормативно-правове регулювання потребує значного покращення та подальшого вдосконалення.

Стрімкий поступ інформаційних і комунікаційних технологій кардинально змінює світ. Вільний та відкритий кіберпростір розширює горизонти свободи та можливостей для кожного, збагачує суспільство в цілому, відкриваючи двері до нового глобального інтерактивного ринку ідей, досліджень та інноваційних рішень. Це стимулює відповідальну та ефективну роботу владних структур, активне залучення громадян до управління державою, вирішення питань місцевого значення, забезпечення публічності та прозорості влади, тим самим сприяючи запобіганню корупції.

Водночас плюси сучасного цифрового простору та розквіт інформаційних технологій спричинили появу нових викликів для національної й світової безпеки. Поруч з випадками ненавмисного характеру збільшується кількість та масштаб кібернападів, які зумовлені інтересами окремих держав, угруповань та особистостей.

Спостерігаємо розповсюдження фактів незаконного збору, накопичення, застосування, ліквідації, розголошення особистих даних, нелегальних фінансових операцій, крадіжок і шахрайств в інтернет-просторі. Кіберзлочинність набуває транскордонного характеру, створюючи серйозну загрозу для інтересів особистості, громади та країни. Зазначені та інші корінні зміни в безпековому полі України, як внутрішньому, так і зовнішньому, диктують необхідність негайного формування національної системи кібербезпеки, як невід'ємної частини системи забезпечення національної безпеки України.

Указом Президента України від 15 березня 2016 року було введено в дію рішення Ради національної безпеки і оборони України, датоване 27 січня 2016 року «Про Стратегію кібербезпеки України» [2]. Її розробка відбулася відповідно до положень Закону України «Про основи національної безпеки України» [3]. Метою Стратегії кібербезпеки України визначено створення необхідного середовища для надійного функціонування кіберпростору, його застосування на благо особистості, соціуму та держави.

Кіберпростір дедалі стає окремою площиною для ведення військових операцій, все більш активно діють відповідні підрозділи збройних сил ключових країн світу. Зважаючи на масштабне використання сучасних інформаційних технологій у безпековому та оборонному секторі, розгортання єдиної автоматизованої системи управління Збройних Сил України робить оборону нашої країни більш вразливою до кібератак.

Зростає кількість кібернападів і кіберзлочинів, об'єктами яких стають інформаційні системи фінансових організацій, транспортних та енергетичних підприємств, а також державних органів, відповідальних за безпеку, оборону та ліквідацію надзвичайних ситуацій. Сучасні технології використовуються не тільки для вчинення звичних злочинів, але й для створення абсолютно нових видів злочинної діяльності, властивих високо інформатизованому суспільству.

Нарешті, 9 травня 2018 року Верховною Радою України був прийнятий Закон України «Про основні засади забезпечення кібербезпеки України» [4].

Актуальність кібербезпеки зростає внаслідок: слабкого захисту критичної інфраструктури державних інформаційних ресурсів; відсутності системного підходу до кіберзахисту критичної інфраструктури; недостатнього розвитку інфраструктури для організаційно-технічного забезпечення кібербезпеки критичної інфраструктури; браком взаємодії між учасниками забезпечення кібербезпеки.

Функції координування та нагляду за діяльністю суб'єктів, які відповідають за кібербезпеку, покладаються на РНБО України. Основними структурами, що гарантують функціонування системи кібербезпеки в Україні є: Міністерство оборони, Служба безпеки, Державна служба спеціального зв'язку та захисту інформації, Національна поліція, Національний банк та інші.

Найперше, забезпечення надійного кіберпростору можливо досягти через:

– формування і приведення державної політики до відповідності стандартам ЄС та НАТО у цій сфері;

– розробка та постійне покращення нормативно-правової бази у сфері кібербезпеки згідно з міжнародними нормами та практиками;

– удосконалення систем кіберзахисту для електронних комунікацій;

– розширення залучення науковців та громадських організацій до процесу розробки критично важливої документації у сфері кібербезпеки;

– організація навчального процесу з цифрової грамотності та безпечного поводження в кіберпросторі. Варто відзначити позитивний досвід Національної академії внутрішніх справ, де на кафедрі інформаційних технологій ННІППП впроваджено навчальну дисципліну «Кібергігієна у професійній діяльності»;

– розбудова інфраструктури електронного зв'язку, доступу до Інтернет;

– активізація міжнародної взаємодії у сфері захисту в кіберпросторі.

Кіберзахист інформаційної інфраструктури країни, а також її електронних інформаційних ресурсів, передбачає реалізацію таких ключових дій: розбудова та функціонування єдиної загальнодержавної комунікаційної мережі державних органів; своєчасна відповідь на кібератаки та інциденти, пов'язані з кібербезпекою; будівництво цілісної системи ситуаційних центрів для державних органів; формування безпечної інтегрованої системи електронних державних реєстрів.

Гарантування стійкого кіберзахисту об'єктів критичної інфраструктури має здійснюватися через: всебічне покращення законодавчої бази у сфері кібербезпеки критично важливих об'єктів; створення державного реєстру об'єктів критичної інформаційної інфраструктури; формування розпорядниками об'єктів критичної інфраструктури власних підрозділів для кіберзахисту; організація співпраці між суб'єктами, які забезпечують кіберзахист критичної інфраструктури, зокрема, в умовах особливого характеру; розроблення та впровадження механізму обміну інформацією між державними органами, приватним сектором і громадянами [5].

Список використаних джерел

1. Про інформацію: Закон України // Відомості Верховної Ради України, 1992, № 48, ст. 650.
2. Про Стратегію кібербезпеки України: Указ Президента України від 15 березня 2016 р. № 96/2016.
3. Про основи національної безпеки України: Закон України від 19.06.2003 № 964-IV // Відомості Верховної Ради України (ВВР), 1997, № 48, ст. 296.
4. Про основні засади забезпечення кібербезпеки України: Закон України від 9 травня 2018 р. № 2163-VIII. URL. https://zakon.rada. gov.ua/laws/show.
5. Дурдинець В.В., Іщенко О.М., Хахановський В.Г. та ін. Система інформаційно-аналітичного забезпечення правоохоронних органів в умовах електронного урядування: монографія, Київ, НАВС, 2018, 273 с.

Хахуцяк Ольга Юріївна, *завідувач кафедри кримінальної юстиції навчально-наукового інституту права та психології НАВС, кандидат юридичних наук, доцент*

ПРАВО СТОРОНИ ЗАХИСТУ НА ДОСТУП ДО МАТЕРІАЛІВ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ ЯК ЕЛЕМЕНТ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ГАРАНТІЯ СПРАВЕДЛИВОГО СУДОЧИНСТВА: ПРАКТИКА ЄСПЛ І НАЦІОНАЛЬНИХ СУДІВ

У сучасних умовах трансформації сектору безпеки та правосуддя України особливого значення набуває забезпечення реального, а не декларативного дотримання права особи на захист у кримінальному провадженні. Саме ефективність реалізації гарантій сторони захисту є одним із критеріїв демократичності держави та рівня довіри до правоохоронної й судової системи. Водночас практика здійснення досудового розслідування свідчить про наявність системних випадків обмеження доступу адвоката до матеріалів кримінального провадження, що негативно впливає як на забезпечення принципу змагальності, так і на загальний стан правової безпеки держави.

Положення ст. 6 Конвенції про захист прав людини і основоположних свобод [1] гарантують кожному право на справедливий судовий розгляд, складовою якого є право на достатній час і можливості для підготовки свого захисту. Європейський суд з прав людини неодноразово наголошував, що право на захист повинно бути «практичним та ефективним, а не теоретичним чи ілюзорним».

Одним із ключових елементів реалізації цього права є своєчасний та повний доступ сторони захисту до матеріалів кримінального провадження. У рішеннях ЄСПЛ у справах Rowe and Davis v. the United Kingdom, Mirilashvili v. Russia, Leas v. Estonia, Matanovic v. Croatia Суд підкреслив, що органи кримінального переслідування зобов'язані надати стороні захисту доступ до всіх матеріалів, які можуть мати значення для доведення невинуватості особи або пом'якшення її відповідальності [2].

У національному законодавстві відповідні гарантії закріплені у ст. 20, 22, 42, 46, 221, 290 КПК України [3]. Водночас практична реалізація зазначених норм часто супроводжується необґрунтованими затягуваннями, формальними відмовами прокурорів або створенням штучних перешкод для ознайомлення адвоката з матеріалами кримінального провадження. Особливої актуальності ця проблема набуває на стадії завершення досудового розслідування та під час підготовчого судового провадження.

Практика ЄСПЛ свідчить, що ненадання стороні захисту достатніх можливостей для ознайомлення з матеріалами справи порушує принцип «рівності сторін» та змагальності процесу. Суд акцентує увагу на тому, що сторона захисту повинна мати реальну можливість ознайомитися з доказами обвинувачення та належним чином підготувати свою правову позицію [4].

У справі Salduz v. Turkey ЄСПЛ наголосив, що доступ до адвоката є однією з фундаментальних гарантій справедливого кримінального провадження, а будь-які обмеження такого доступу можуть призвести до порушення ст. 6 Конвенції [5].

Аналіз судової практики Верховного Суду також свідчить про формування підходу, відповідно до якого недотримання вимог ст. 290 КПК України щодо відкриття матеріалів може бути підставою для визнання доказів недопустимими. Верховний Суд неодноразово звертав увагу на те, що сторона обвинувачення не має права вибірково визначати обсяг матеріалів, які підлягають відкриттю стороні захисту, оскільки це суперечить принципам справедливого судового розгляду та змагальності сторін.

Крім процесуального аспекту, проблема доступу адвоката до матеріалів кримінального провадження має безпосередній зв'язок із забезпеченням національної безпеки. В умовах воєнного стану, зростання кількості кримінальних проваджень щодо воєнних злочинів, колабораційної діяльності, злочинів проти основ національної безпеки особливого значення набуває баланс між інтересами держави та дотриманням фундаментальних прав людини. Порушення права на захист навіть у найбільш резонансних категоріях справ створює ризики визнання Україною порушень Конвенції та підриває авторитет національної системи правосуддя на міжнародному рівні.