УДК 351.86/004.85

КУДІНОВ С.С., *доктор юридичних наук, професор*

ФОРМУВАННЯ АНТИТЕРОРИСТИЧНИХ КОМПЕТЕНТНОСТЕЙ ФАХІВЦІВ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ

DOI...

Анотація. *Статтю присвячено питанням протидії тероризму в кіберпросторі. Акцентовано увагу на актуальності терористичної загрози в Україні та світі. Охарактеризовано національну систему кібербезпеки, існуючі підходи до підготовки фахівців для неї та міжнародний досвід у цій сфері. Обґрунтовано необхідність формування у фахівців системи антитерористичної компетентності, описано її зміст на підставі міжнародного досвіду, визначено шляхи запровадження такої підготовки в Україні.*

Ключові слова: *тероризм, терористична діяльність, кіберпростір, кібертероризм, національна система кібербезпеки, антитерористична компетентність.*

Summary. *The article is devoted to topical issues of combating terrorism in cyberspace. Attention is focused on the relevance of terrorist threats to Ukraine and the world. The national cyber security system, existing approaches to training specialists for it and relevant international experience in this field are characterized. Taking into account the existence of a terrorist threat, the need for the formation of anti-terrorist competence among specialists of the specified system is substantiated, its content is described, and ways of introducing such training in Ukraine are determined on the basis of international experience.*

Keywords: *terrorism, terrorist activity, cyberspace, cyberterrorism, national cyber security system, anti-terrorist competence.*

Постановка проблеми. Стратегія кібербезпеки України закріплює, що для подальшої розбудови національної системи кібербезпеки на засадах стримування, кіберстійкості, взаємодії необхідним є посилення спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням, нейтралізації розвідувально-підривної діяльності, мінімізації загроз кіберзлочинності та кібертероризму (стримування), також закріплює необхідність проведення в Україні докорінної реформи системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки [10].

На жаль, здобутки науково-технічного прогресу призвели до того, що сьогодні кіберпростір вже використовується для здійснення терористичної діяльності, що в свою чергу обумовлює необхідність перегляду змісту підходів до формування професійних компетентностей фахівців національної системи кібербезпеки України.

Результати аналізу наукових публікацій. Питання боротьби з тероризмом були предметом наукових розвідок зарубіжних та вітчизняних науковців, а саме: В. Антипенко, В. Буткевича, Г. Вордлоу, М. Головатого, М. Гуцало, В. Денисова, В. Ємельянова, І. Зволінського, А. Змієвського, В. Крутова, В. Кудрявцева, І. Лазарєва, Дж. Ламберт, У. Латипов, В. Ліпкана, Б. Леонова, І. Мусієнка, А. Носача, В. Панова, І. Рижова, М. Сенченка, У. Сломансона, І. Хижняка, І. Шкурата та ін.

Розробці питань безпечного кіберпростору, протидії кібертероризму, підготовки фахівців для національної системи кібербезпеки України присвячені праці Л. Арсеновича, В. Богуша, В. Бурячка, С. Гнатюка, Ю. Даніка, І. Діордиці, О. Довганя., І. Дороніна., Д. Дубова., О. Євсюкової, С. Мельника, В. Толубка, С. Толюпи, В. Шеломенцева та ін.

Разом з тим, в умовах бурхливого розвитку кіберпростору, його значення для існування людства, постійної терористичної загрози, питання вдосконалення підготовки фахівців для національної системи кібербезпеки, запровадження їх антитерористичної підготовки, як одного з засобів протидії тероризму, потребують подальших наукових розвідок.

Метою статті є обґрунтування необхідності формування антитерористичної компоненти в підготовці фахівців національної системи кібербезпеки України.

Виклад основного матеріалу. На сьогодні питання якісної підготовки фахівців з кібербезпеки для органів державної влади України є одним із пріоритетних завдань, що визначені нормативно-правовими актами України у сфері забезпечення кібербезпеки, як однієї із важливих складових сфер національної безпеки і оборони держави в умовах ведення війни проти України [1, с. 24].

Слід відзначити, що характерною особливістю сучасної теорії та практики підготовки кадрів для сектору безпеки і оборони у провідних країнах Заходу є те, що владні структури повною мірою усвідомлюють надзвичайну важливість якісної професійної підготовки спецслужбовців, а також обов'язковість належного матеріального та морально-психологічного супроводу цього процесу. Для урядів-країн ЄС і НАТО аксіомою є твердження, що наявність добре підготовлених кадрів – неодмінна умова якісного функціонування силових структур. Провідні країни світу накопичили тривалий досвід формування й удосконалення систем підготовки кадрів для сектору безпеки і оборони. Слід зауважити, що відповідні національні системи мають характерні особливості та розбудовуються на основі власних пріоритетів і завдань, з урахуванням потреб внутрішньої та зовнішньої безпекової ситуації [12, с. 68].

Сьогодні підготовка кадрів для національної системи кібербезпеки України є складовою загальнодержавної системи освіти і включає в себе органи управління, мережу вищих спеціальних навчальних закладів і спеціальних навчальних підрозділів вищих навчальних закладів, а також підбір та перепідготовка, підвищення кваліфікації кадрів з числа випускників цивільних навчальних закладів, що володіють необхідною компетентністю для подальшого проходження служби (роботи) в секторі безпеки і оборони України.

Останній підхід відповідає і практиці багатьох країн ЄС і НАТО, де навчальні заклади, які здійснюють підготовку кадрів для правоохоронних і розвідувальних органів, зазвичай орієнтовані на професійну підготовку осіб, котрі вже отримали вищу освіту в цивільних чи військових ЗВО. Ці заклади освіти зі специфічними умовами навчання, як правило, проводять короткострокові навчальні курси, приділяючи особливу увагу розвиткові у слухачів (курсантів) необхідних практичних навичок [12, с. 68].

Доволі цікавою, з цього приводу, є позиція І.В. Діордиці, про те, що фахівцями у сфері кібербезпеки є не тільки випускники технічних університетів, а й правники, аналітики, судові експерти та ін. категорії працівників, які за своїм посадовими обов'язками повинні забезпечувати дотримання інформаційних прав і свобод людини, упереджувати або нейтралізовувати протиправні діяння в комп'ютерному просторі, вчиняти процесуальні дії, які мають на меті покарання правопорушників [5, с. 420].

В Україні підготовку бакалаврів та магістрів за спеціальностями галузі знань "Інформаційні технології" здійснюють 160 закладів вищої освіти. З них: 123 заклади вищої освіти, які здійснюють підготовку бакалаврів та магістрів за спеціальностями галузі знань "Інформаційні технології", є державними (76,7 %), та 37 закладів вищої освіти, які забезпечують підготовку таких фахівців у приватному порядку (23,3 %) [1, с. 20-21].

Баррі Бузан звертає увагу на те, що з розвитком сучасних технологій, поширенням світом таких небезпечних явищ, як міжнародний тероризм, кіберзлочинність тощо, освітні програми у сфері безпеки "набувають більш широких, глибоких і складних підходів щодо того, як інтерпретувати будь-яку подію або проблему" [15, с. 255].

З цього приводу фахівці Національного інституту стратегічних досліджень, зазначають, що протидія загрозам нового, гібридного типу здебільшого належить до компетенції правоохоронних органів і спеціальних служб. Тому, вимоги до їхньої діяльності підвищуються, а освітній процес при підготовці кадрів для правоохоронних органів і спецслужб закономірно стає більш динамічним і різноманітним [12, с. 68].

Відповідно до положень чинного законодавства 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 [6].

Основними з яких, відповідно до ст. 8 Закону України "Про основні засади забезпечення кібербезпеки України" 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 [6].

На думку професора О.В. Діденка, компетентність як комплексна особистісна категорія означає практичну готовність і здатність людини діяти в певній галузі; вона охоплює теоретичні знання, уявлення, уміння, навички, мотиви, цінності; передбачає наявність досвіду діяльності [4].

Вочевидь, що професійна компетентність фахівця національної системи кібербезпеки нерозривно пов'язана, з одного боку, з наявністю знань, вмінь і навичок щодо загроз кібернетичній безпеці України, їх ідентифікації та нейтралізації, взаємодії відповідних суб'єктів її забезпечення тощо, а з іншого – зі станом її захищеності від реальних та потенційних загроз.

Тероризм залишається глобальним лихом: він зачіпає людей різного віку, культур, релігій та національностей. Про це заявив, звертаючись до учасників наради в Нью-Йорку Генеральний секретар ООН Антоніу Гутерриш у січні 2023 року [13]. Наявність терористичної загрози національній безпеці визначена в стратегічних безпекових документах нашої крани, зокрема: Стратегії національної безпеки України, 14.09.20 р. [11]; Стратегія воєнної безпеки України, 25.03.21 р. [9]; Концепція боротьби з тероризмом, 05.03.19 р. [14], в свою чергу загроза кібертероризму визначена Стратегією кібербезпеки 26.08.21 р. [10]. При цьому, фахівці ООН з протидії тероризму відзначають, що терористи все активніше використовують новітні технології [13].

Одним із небезпечних проявів тероризму в сучасному світі є кібертероризм. Який в чинному законодавстві визначений, як терористична діяльність, що здійснюється у кіберпросторі або з його використанням [6].

Термін "кібертероризм" був запропонований у 1980-х р. співробітником американського Інституту безпеки і розвідки (Institute for Security and Intelligence) Баррі Колліном, який використав його в контексті тенденції до переходу тероризму від фізичного до віртуального, породжуючого перетин та злиття цих світів [16].

Розкриваючи його сутність, С. Гнатюк визначає його як різновид тероризму, що полягає у свідомому та цілеспрямованому застосуванні ресурсів інформаційних систем для реалізації терористичних дій у кіберпросторі, а також для досягнення інших суміжних цілей в інтересах терористичних угруповань [3, с. 122].

До основних причин його виникнення зазначений науковець відносить: різке збільшення продуктивності та одночасне здешевлення сучасних обчислювальних засобів, що робить їх загальнодоступними і значно розширює множину потенційних кіберзагроз, а також відсутність чітких кордонів у кіберпросторі, що нівелює відмінність між зовнішніми та внутрішніми джерелами загроз кібербезпеці держави. Крім того, кіберпростір дає можливість зловмисникам маніпулювати інформацією і її сприйняттям суспільством на власний розсуд, а також дозволяє реалізувати терористичні дії з безпрецедентною оперативністю і зробити завдання ідентифікації зловмисників дуже складним угруповань [3, с. 124].

Слід погодитися з позицією фахівців, які вказують, що специфіка фахової підготовки й формування професійної компетентності майбутніх фахівців з кібербезпеки зумовлює застосування інтегрованого підходу, що базується на міжпредметних зв'язках фахових і фундаментальних навчальних дисциплін та ефективного розподілу навчальних модулів в системі професійної підготовки з урахуванням модернізаційних освітніх змін, педагогічної інноватики та застосуванні інноваційних освітніх технологій для формування комплексної готовності до реалізації фахових компетенцій з кібербезпеки [8].

Антитерористична компетентність є інтегративною здатністю людини успішно діяти в умовах терористичного акту. Її змістовними складовими є необхідні знання, вміння, навички, мотиви, світогляд й соціальні настанови; а для суб'єктів, що здійснюють боротьбу з тероризмом, або залучаються до неї – професійно-важливі знання, вміння, навички, мотиви, якості та світогляд, соціальні настанови, професійна готовність до ефективних дій в умовах терористичної загрози [7].

Вона, як засіб протидії тероризму, в тому числі і в кіберпросторі, є засобом реакції суспільства на глобальну загрозу людству – тероризм.

Вочевидь компетентності фахівців національної системи кібербезпеки України повинні дозволяти їм нейтралізовувати загрози кібербезпеці нашої країни. Зокрема, фахівці, які займалися дослідженням моделей підготовки фахівців для цієї системи, вказують, що результатами їх навчання у закладах вищої освіти України, окрім іншого повинно бути – володіння достатніми науковими знаннями щодо теоретичних та методологічних основ запобігання кібернетичній злочинності, кібернетичному тероризму, кібернетичним конфліктам і війнам на основі впровадження методів та експлуатації засобів превентивного забезпечення кібернетичної безпеки [2, с. 284].

Розглядаючи безпосередньо питання змісту антитерористичної компетентності, необхідно в першу чергу виходити з характеристики самої проблеми:

По-перше, тероризм – є ідеологією, ідеєю яка виправдовує, обумовлює доцільність застосування терористичних методів.

По-друге, небезпека тероризму полягає у двох основних складових: безпосередньо вражаючий фактор (вибух, постріл, застосування зброї масового знищення, транспортного засобу, шкідливої програми тощо), а також інформаційно-психологічна атака, що має метою створення обстановки хаосу, страху (це публічний спосіб вчинення злочину, розповсюдження інформаційних, відео-, фотоматеріалів, що мають залякувати людей) задля досягнення мети терористичної діяльності, або окремого акту (наприклад, зміна політичного курсу країни, звільнення поплічників терористів, отримання викупу за заручників тощо).

По-третє, основу протидії цьому явищу становить його нормативно-правове визначення та заборона, а також сформована державна система протидії йому (що включає визначення уповноважених органів, їх компетенції, форм і методів роботи, а також особливості взаємодії між елементами системи та ін. органами (в т.ч. державними та міжнародними, підприємствами, установами, організаціями та цивільними особами).

По-четверте, сучасні стратегії боротьби з тероризмом, виходять з пріоритету захисту прав і свобод людини, суспільства та держави, не порушення прав людини у протидії тероризму.

Таким чином, зміст антитерористичної підготовки фахівців національної системи кібербезпеки повинен охоплювати питання:

- розуміння тероризму, його сутності та загрози для існування людства, його ідентифікації;
- причин виникнення тероризму, радикалізації суспільства, сутності та складових загроз терористичного характеру; існуючих стратегій боротьби з тероризмом, їх особливостей та характеристик,
- поняття та складових антитерористичної безпеки тощо;
- державної системи боротьби з тероризмом, її структурних елементів, їх повноважень, порядку взаємодії, в тому числі з цивільним населенням, правил антитерористичної безпеки, відповідальності за здійснення терористичної діяльності тощо;
- поведінки в разі загрози терористичного характеру та антитерористичної операції, зокрема поведінки та забезпечення фізичного самозахисту особи у разі терористичної загрози та після терористичного акту (вдома, на роботі, у транспорті, в Інтернеті), психологічної саморегуляції тощо;
- моніторингу та аналізу ризиків і загроз терористичного характеру, планування коригуючих впливів, починаючи від виявлення та ідентифікації терористичної загрози, визначення її небезпеки для себе, оточуючих, колег і закінчуючи способами нейтралізації терористичної загрози.

Висновки.

Існування терористичної загрози в кіберпросторі обумовлює необхідність формування антитерористичної складової професійної компетентності фахівців національної системи кібербезпеки. Така компетентність може формуватися під час навчання у відповідних закладах освіти, що здійснюють підготовку фахівців для національної системи кібербезпеки або шляхом проходження відповідних курсів підвищення кваліфікації. Зміст антитерористичної підготовки зазначених фахівців повинні складати питання поняття тероризму, причин його виникнення, його правової характеристики, існуючих систем та стратегій протидії йому, взаємодії з відповідними суб’єктами, поведінки в умовах терористичної загрози, моніторингу, ідентифікації та нейтралізації терористичної загрози.

Використана література

1. Арсенович Л.І. Стан організації професійної підготовки фахівців із кібербезпеки в умовах особливого періоду. *Дніпровський науковий часопис публічного управління, психології, права*. Вип. 4. 2022. С. 18-26.

2. Бурячок В.Л., Богуш В.М., Борсуковський Ю.В., Складанний П.М., Борсуковська В.Ю. Модель підготовки фахівців у сфері інформаційної та кібернетичної безпеки в закладах вищої освіти України. *Інформаційні технології і засоби навчання*, 2018. Т. 67. № 5. С. 277-288. ISSN: 2076-8184.

3. Гнатюк С.О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Безпека інформації*. 2013. Т. 19. № 2. С. 118-129.

4. Діденко О.В. Особливості впровадження компетентнісного підходу у професійну підготовку майбутніх офіцерів у ВНЗ. *Вісник Національної академії Державної прикордонної служби України*. 2014. Вип. 3. URL: http://nbuv.gov.ua/UJRN/Vnadps_2014_3_6

5. Діордіца І.В. Кібербезпекова політика України: стан та пріоритетні напрями забезпечення: монографія. Херсон: Видавничим дім "Гельветика", 2017. 548 с.

6. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. URL: https://zakon. rada.gov.ua/laws/show/2163-19#Text

7. Кудінов С.С. Правова політика з формування антитерористичної компетентності в Україні: монографія. Одеса: Видавець Букаєв Вадим Вікторович, 2019, 268 с.

8. Мельник С.В., Воскобойников С.О, Ступак Д.Є. Оптимізація фахової підготовки майбутніх фахівців з кібербезпеки на основі інноваційної педагогіки та інтегрованого підходу в системі реалізації ключових компетенцій безпеки в інформаційному суспільстві. *Витоки педагогічної майстерності.* 2018. Вип. 21. ISSN: Print 2075 – 146 X. Online 2616-6623.

9. Стратегія воєнної безпеки України: Указ Президента України від 25.03.21 р. № 121/2021. URL: https://zakon.rada. gov.ua/laws/ show/121/2021#n2

10. Стратегія кібербезпеки України: Указ Президента України від 26.08.21 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12

11. Стратегія національної безпеки України: Указ Президента України від 14.09.20 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/ show/392/2020#Text

12. Сьомін С.В., Резнікова О.О. Проблеми реформування системи підготовки кадрів для сектору безпеки і оборони України. *Стратегічна панорама*. 1' 2017. С. 67-73.

13. Терористи активно опановують нові технології, попереджають в ООН. URL: https://news. un.org/ru/story/2023/01/1436982

14. Про Концепцію боротьби з тероризмом в Україні: Указ Президента України від 05.03.19 р. № 53/2019. URL: https://zakon.rada.gov.ua/laws/show/53/2019#Text

15. Buzan B., Hansen L. The evolution of international security studies. New York: Cambridge University Press, 2009. 383 p.

16. Collin B. The Future of Cyberterrorism. *Crime & Justice International Journal*. 1997. Vol. 13. Вип. 2.1. P. 5.1-26.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~