УДК 327.7:061.1 DOI: https://doi.org/10.33990/2070-4011.62.2020.205817

Арсенович Леонід Антонович
заступник начальника управління – начальник відділу Департаменту кадрової роботи та управління персоналом Адміністрації Державної служби спеціального зв'язку та захисту інформації України, аспірант Національної академії державного управління при Президентові України
ORCID: 0000-0001-7081-2838
e-mail: arsen-leon@ukr.net

ОРГАНІЗАЦІЯ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ФАХІВЦІВ ІЗ КІБЕРБЕЗПЕКИ ОСНОВНИМИ СУБ'ЄКТАМИ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ: ПРАКТИЧНИЙ АСПЕКТ

Проведено аналіз нормативно-правового забезпечення підготовки фахівців із кібербезпеки та надано характеристику системі підготовки та підвищення кваліфікації фахівців із кібербезпеки основних суб'єктів національної системи кібербезпеки. Виявлено проблемні питання щодо підготовки та підвищення кваліфікації фахівців із кібербезпеки основних суб'єктів національної системи кібербезпеки, що уповільнюють впровадження інформаційних технологій в усіх сферах суспільного життя та діяльності. Сформульовано пропозиції основним суб'єктам національної системи кібербезпеки та Національному координаційному центру кібербезпеки, які беруть участь у професійній підготовці фахівців із кібербезпеки, для подальшого використання у практичній діяльності та для удосконалення відповідної нормативно-правової бази.

Ключові слова: інформаційна безпека; інформаційні технології; кібербезпека; кіберзахист; професійна підготовка; Стратегія кібербезпеки.

Постановка проблеми. В умовах розбудови цифрового світу та розвитку інформаційних технологій особливого значення набувають проблеми професійної підготовки спеціалістів ІТ-сфери, насамперед фахівців із кібербезпеки основних суб'єктів національної системи кібербезпеки.

Зовнішні та внутрішні загрози у безпековому середовищі України актуалізують потребу підвищення рівня професійної компетенції фахівців, які в умовах протидії збройній агресії Російської Федерації опікуються питаннями кібербезпеки та кіберзахисту державних інформаційних ресурсів.

Рівень підготовки військовослужбовців та осіб начальницького складу основних суб'єктів національної системи кібербезпеки (Державна служба спеціального зв'язку та захисту інформації України (далі – СБ України), Національна поліція України, Служба безпеки України, Міністерство оборони України, Генеральний штаб Збройних сил України (далі – ГШ ЗС України) та розвідувальні органи України), які відповідають за створення національної системи кібербезпеки, повинен відповідати не лише сучасним потребам

розвитку інформаційного суспільства, але й забезпечити здатність фахівців із кібербезпеки знаходити рішення у складних ситуаціях під час виконання своїх службових обов'язків. Зазначене потребує якісних змін, насамперед нормативно-правового забезпечення зазначеної сфери. Зміни у законодавстві є однією з передумов підвищення ефективності процесу навчання, створення умов для підвищення рівня професійної підготовки фахівців із кібербезпеки та реалізації цілеспрямованого процесу їх особистісного та професійного зростання.

Організація підготовки та підвищення кваліфікації фахівців із кібербезпеки є проблемними питаннями забезпечення кібербезпеки України. У контексті проведення реформ у всіх сферах життєдіяльності українського суспільства якісна підготовка фахівців із кібербезпеки основних суб'єктів національної системи кібербезпеки набуває особливої актуальності та потребує окремої уваги керівників зазначених суб'єктів.

Аналіз останніх досліджень і публікацій. У ході аналізу встановлено, що насамперед розбудова системи підготовки та підвищення кваліфікації кадрів для структур, які гарантують безпеку країни у сфері кібербезпеки шляхом ефективних реформ, є одним із напрямів реалізації Стратегії кібербезпеки України та Концепції розвитку сектору безпеки і оборони України.

Проведений аналіз доводить, що для України формування нової культури безпеки зі збереженням професійної підготовки кадрів, підвищення кваліфікаційного рівня персоналу та забезпечення його високої мотивації професійної діяльності у галузі кібербезпеки є справою державного рівня. Вивчення наукових здобутків та практик щодо підготовки фахівців із кібербезпеки в країнах Європейського Союзу дає змогу визначити завдання та шляхи подальшого удосконалення системи підготовки фахівців цієї галузі знань.

Як свідчать останні дослідження і публікації, проблеми професійного розвитку фахівців із кібербезпеки є малодослідженими. Так, І. Діордіца у своїх статтях досліджує питання стандартизації підготовки фахівців із кібербезпеки та здійснює аналіз стану підготовки фахівців у сфері кібернетичної безпеки станом на 2015 – 2016 рр. [1, 2]. С. Мельник у науковій роботі визначає концептуальні основи організації професійної підготовки майбутніх фахівців із кібербезпеки у закладах вищої освіти [3]. А група науковців у складі В. Бурячка, І. Пархомея, М. Степанова та В. Толубка у своїй статті вивчає проблемні питання та актуальні завдання підготовки фахівців із кібернетичної безпеки галузі знань "Інформаційні технології" [4].

Водночас доцільно зазначити, що питання організації професійної підготовки фахівців із кібербезпеки на сьогодні в контексті реалізації Стратегії кібербезпеки України та інших нормативно-правових актів залишилося поза увагою комплексних наукових досліджень. На практиці це призводить до недооцінення ролі навчання особового складу основних суб'єктів національної системи кібербезпеки, що є одним із пріоритетів та напрямів забезпечення кібербезпеки України.

Виокремлення невирішених раніше частин загальної проблеми. Метою статті є визначення проблемних питань професійної підготовки фахівців із кібербезпеки. Досягнення визначеної мети потребує надання характеристики системі підготовки та підвищення кваліфікації фахівців із кібербезпеки основних суб'єктів національної системи кібербезпеки.

Виклад основного матеріалу. Швидкий розвиток інформаційних технологій поступово трансформує світ. Відкритий кіберпростір розширює свободу людей і можливості суспільства, створює новий і цікавий ринок ідей, досліджень та інновацій, стимулює роботу влади і керівників усіх рівнів, активне залучення громадян до управління державою та вирішення місцевих питань, сприяє запобіганню корупції тощо.

Гібридна війна з боку Російської Федерації та інші зміни у безпековому середовищі України вимагають невідкладного створення національної системи кібербезпеки як складової системи забезпечення національної безпеки України.

На сучасному етапі підготовка висококваліфікованих кадрів залишається ключовим елементом повноцінної життєдіяльності держави. Цей процес характеризується поєднанням потреб суспільства з сучасними інформаційними технологіями із подальшим закріпленням на рівні нормативно-правових актів.

Проблеми забезпечення кібербезпеки пов'язані не лише із застарілістю та/або неефективністю програмно-апаратних рішень, а й із недостатньою кваліфікацією спеціалістів із кібербезпеки. Кадрова проблема стала для індустрії кібербезпеки глобальною і має, до того ж, тенденцію до поглиблення – світова потреба у фахівцях із кібербезпеки нині в середньому у 12 разів вища за потребу в інших IT-спеціалістах. При цьому значна нестача фахівців у сфері кібербезпеки вже призводить до зниження їх професійного рівня: 37% роботодавців світу незадоволені низькою підготовкою фахівців у цій галузі. Про таке свідчать матеріали аналітичної доповіді Національного інституту стратегічних досліджень "Кібербезпека в умовах розгортання четвертої промислової революції (industry 4.0): виклики та можливості для України" від 15.05.2019 р. [5].

Забезпечення кібербезпеки України як стану захищеності інтересів людини, суспільства та держави в кіберпросторі, що досягається застосуванням сукупності правових, організаційних, інформаційних заходів, має базуватися, зокрема, й на дійовій організації професійної підготовки фахівців управління кібербезпекою.

Питання професійної підготовки фахівців із кібербезпеки висвітлюється в низці нормативно-правових актів, підготованих і затверджених Верховною Радою, Президентом України та Кабінетом Міністрів України. Водночас поняття "професійна підготовка" ми розглядаємо як участь фахівців основних суб'єктів національної системи кібербезпеки в організації і проведенні кібернавчань та тренінгів у сфері забезпечення кібербезпеки, підготовку фахівців освітньо-кваліфікаційних рівнів бакалавра і магістра за державним замовленням,

створення системи підготовки кадрів у сфері кібербезпеки для потреб основних суб'єктів національної системи кібербезпеки.

Умовно можна виділити декілька документів, які "закладають фундамент" організації підготовки фахівців із кібербезпеки основними суб'єктами національної системи кібербезпеки. Зокрема, це закони та підзаконні нормативно-правові акти, які регламентують пріоритети, забезпечення, принципи та напрями навчання фахівців із кібербезпеки (Закон України "Про основні засади забезпечення кібербезпеки України" [6], Стратегія національної безпеки України [7], Стратегія кібербезпеки України [8], Положення про Національний координаційний центр кібербезпеки [9]) та які безпосередньо затверджують заходи з реалізації Стратегії кібербезпеки України (розпорядження Кабінету Міністрів України на відповідний рік).

Першим нормативно-правовим актом, у якому йдеться про створення системи підготовки кадрів у сфері кібербезпеки, є Стратегія національної безпеки України, затверджена Указом Президента України № 287 від 26.05.2015 р. Стратегією визначено, що підготовка фахівців із кібербезпеки є пріоритетом забезпечення кібербезпеки і безпеки інформаційних ресурсів, який є одним із основних напрямів державної політики національної безпеки України.

Стратегія національної безпеки України стала основою для розроблення інших документів стратегічного планування у сфері забезпечення національної безпеки: Стратегії кібербезпеки України, затвердженої Указом Президента України № 96 від 15.03.2016 р.; Положення про Національний координаційний центр кібербезпеки, затвердженого Указом Президента України № 242 від 07.06.2016 р.

Стратегія кібербезпеки України формує підґрунтя для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави та визначає концептуальні основи побудови системи кібербезпеки України. У наведеному документі зазначено, що кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації, вимога щодо захисту якої встановлена законом, має полягати, насамперед, у підвищенні обізнаності працівників державних органів у сфері інформаційної безпеки та кібербезпеки, проведенні відповідних тренінгів, навчань.

Національний координаційний центр кібербезпеки, який є робочим органом Ради національної безпеки і оборони України, також передбачає навчання особового складу основних суб'єктів національної системи кібербезпеки. Так, одним із основних завдань цього центру є участь в організації і проведенні міжнаціональних і міжвідомчих кібернавчань та тренінгів у сфері забезпечення кібербезпеки, розроблення відповідних методичних документів і рекомендацій.

Як бачимо, у наведених документах надаються загальні напрями професійної підготовки фахівців із кібербезпеки. Завдання, які детальніше

передбачають організацію та здійснення основними суб'єктами національної системи кібербезпеки заходів із підготовки кадрів у сфері кібербезпеки, були визначені щорічними планами заходів із реалізації Стратегії кібербезпеки України, що затверджувалися розпорядженнями Кабінету Міністрів України протягом 2016 – 2018 рр. Аналіз стану виконання таких планів, проведений нами, засвідчив, що питання професійної підготовки фахівців із кібербезпеки залишається невиконаним або ж і виконаним, але не в повному обсязі.

Так, План заходів на 2016 рік із реалізації Стратегії кібербезпеки України, затверджений Розпорядженням Кабінету Міністрів України № 440-р від 24.06.2016 р. [10], План заходів на 2017 рік з реалізації Стратегії кібербезпеки України, затверджений Розпорядженням Кабінету Міністрів України № 155-р від 10.03.2017 р. [11] та План заходів на 2018 рік з реалізації Стратегії кібербезпеки України, затверджений Розпорядженням Кабінету Міністрів України № 481-р від 11.07.2018 р. [12], передбачали організацію та проведення основними суб'єктами національної системи кібербезпеки конференцій, семінарів, форумів, засідань за круглим столом, тренінгів, навчань із питань інформаційної безпеки, кібербезпеки та захисту інформації в кіберпросторі на державному та міжнародному рівнях.

Результати організації, проведення та участі у таких заходах протягом 2016 – 2018 рр. наведено в табл. 1.

Таблиця 1

Організація, проведення та участь у навчальних (освітніх) заходах основних суб'єктів національної системи кібербезпеки з питань інформаційної безпеки, кібербезпеки, кіберзахисту та захисту інформації в кіберпросторі протягом 2016 – 2018 рр.

Основні суб'єкти національної системи кібербезпеки									
Адміністрація Держспецзв'язку	Служба безпеки України	Міністерство оборони України	Генеральний штаб Збройних сил України	Міністерство закордонних справ України	Міністерство внутрішніх справ України	Національна поліція України	Національний банк України	Національна академія наук України	Інші зацікавлені органи виконавчої влади
1	2	3	4	5	6	7	8	9	10
2016 р.									
На державному рівні									
0/4	1/4	2/4	0/4	0/4	0/4	0/4	0/4	0/4	0/4
На міжнародному рівні									
0/13	2/13	2/14	0/13	0/13	0/13	0/13	0/13	0/13	0/13
2017 р.									
На державному рівні									
3/3	0/3	0/3	0/3	0/3	0/3	0/3	0/3	0/3	0/3
На міжнародному рівні									
0/14	2/15	0/14	0/14	0/14	0/14	0/15	0/14	0/14	1/16

Закінчення табл. 1

1	2	3	4	5	6	7	8	9	10
2018 р.									
На державному рівні									
2/2	1/2	0/1	0/1	0/1	0/1	1/2	0/1	1/3	2/4
На міжнародному рівні									
2/2	2/2	0/2	0/2	0/2	0/2	1/6	0/2	0/2	0/2
Загалом за 2016 – 2018 рр.									
На державному рівні									
5/9	2/9	2/8	0/8	0/8	0/8	1/9	0/8	1/10	2/11
На міжнародному рівні									
2/16	6/17	2/17	0/16	0/16	0/16	1/21	0/16	0/16	1/18

Як видно з табл. 1, основна увага здебільшого була зосереджена не на організації та проведенні навчальних (освітніх) заходів із питань інформаційної безпеки, кібербезпеки, кіберзахисту та захисту інформації в кіберпросторі, а на участі у таких заходах, які були організовані іншими державними та приватними інституціями. До того ж, як констатують вищезазначені дані, участь основними суб'єктами національної системи кібербезпеки здебільшого бралася у освітніх заходах, що організовувалися міжнародними партнерами, а не державними органами. Це участь у щорічній конференції Форуму команд реагування на комп'ютерні інциденти FIRST (м. Сеул, Республіка Корея), проєкті HATO Multinational Cyber Defence Education and Training в межах ініціативи Smart Defence, міжнародних командно-штабних навчаннях "Непорушна стійкість 2018/Coherent resilience 2018 (COREX 2018)" тощо.

Виникає питання, чому присутня зазначена тенденція? З якої причини протягом 2016 – 2018 рр. основними суб'єктами національної системи кібербезпеки було організовано лише 13 офіційних освітніх заходів на державному рівні? Однією з причин є відсутність у складі міністерств та відомств, що є основними суб'єктами національної системи кібербезпеки, окремих підрозділів (секторів, відділів, управлінь), які б опікувалися питаннями підготовки та підвищення кваліфікації особового складу, насамперед із питань кібербезпеки, кіберзахисту, інформаційної безпеки та захисту інформації в кіберпросторі. Так, наприклад, в Адміністрації Держспецзв'язку питаннями підготовки та підвищення кваліфікації особового складу, відповідно до функціональних обов'язків, опікується лише один фахівець (при загальній кількості співробітників Держспецзв'язку у більш ніж 7 тис. осіб), що, своєю чергою, не може позитивно позначатися на організації освітньої діяльності цієї служби.

Наступним аспектом, який не менш вагомий при організації освітніх заходів, є відповідне державне замовлення на підготовку фахівців із

кібербезпеки. Нині в масштабах держави не існує чіткого механізму визначення такої потреби, насамперед за диференційними ознаками відповідно до ступенів вищої освіти. Про це наочно свідчать кількісні показники, що систематизовані за даними з обсягів державного замовлення на підготовку фахівців галузі знань "Інформаційні технології" за спеціальністю "Кібербезпека" упродовж 2017 – 2019 рр. (табл. 2).

Таблиця 2

Розподіл фахівців за рівнями вищої освіти залежно від замовлення роботодавців упродовж 2017 – 2019 рр.

Замовник	Бакалавр (прийом)		Магістр (прийом)	
	Усього	Денна форма	Усього	Денна форма
2017 р.				
МВС України	38	38	1	1
ДСНС України	13	13	1	1
Міноборони України	43	28	15	15
МОН України	940	940	450	450
Адміністрація Держспецзв'язку	60	60	21	21
Загалом	**1094**	**1079**	**488**	**488**
2018 р.				
МВС України	60	60	3	3
ДСНС України	10	10	3	3
Міноборони України	57	37	22	22
МОН України	960	960	486	486
Адміністрація Держспецзв'язку	50	50	25	25
СЗР України	4	4	-	-
Загалом	**1141**	**1121**	**539**	**539**
2019 р.				
МВС України	31	31	-	-
ДСНС України	6	6	-	-
Міноборони України	59	39	14	14
МОН України	980	980	480	460
Адміністрація Держспецзв'язку	60	60	25	25
Загалом	**1136**	**1116**	**519**	**499**
за 2017 – 2019 рр.				
МВС України	129	129	4	4
ДСНС України	29	29	4	4
Міноборони України	159	104	51	51
МОН України	2880	2880	1416	1396
Адміністрація Держспецзв'язку	170	170	71	71
СЗР України	4	4	-	-
Загалом	**3371**	**3316**	**1546**	**1526**

Як видно з табл. 2, потужний акцент у підготовці фахівців із кібербезпеки протягом останніх трьох років робиться на підготовці бакалаврів. Такий підхід є доволі "дивним" із урахуванням того, що 27 червня 2017 р. в Україні відбулася наймасовіша кібератака на IT-системи фінансового, енергетичного, транспортного та інших секторів критичної інфраструктури, результати якої повинні були б "підштовхнути" принаймні основні суб'єкти національної системи кібербезпеки до свідоміших дій щодо подальшого державного замовлення фахівців із кібербезпеки. Виникає питання, наскільки компетентність бакалавра дасть змогу протистояти таким загрозам? Чому основними суб'єктами національної системи кібербезпеки недооцінюється державне замовлення на підготовку магістрів? Зазначена ситуація, яка склалася стосовно підготовки магістрів за спеціальністю "Кібербезпека" протягом 2017 – 2019 рр., є ризикованою і небезпечною для основних суб'єктів національної системи кібербезпеки та держави загалом. Тому надалі необхідно порушувати питання щодо збільшення кількості магістрів, які готуються за спеціальністю "Кібербезпека".

Окрім цього, необхідно виділити кількість фахівців із кібербезпеки, яку замовляли основні суб'єкти національної системи кібербезпеки та інші органи протягом вищезазначених років для своїх потреб. Так, протягом 2017 – 2019 рр. Міноборони, МВС, ДСНС, Адміністрацією Держспецзв'язку та СЗР замовлено 491 фахівець-бакалавр, що становить 14,5% від загальної кількості замовлених бакалаврів, та 130 фахівців-магістрів, що дорівнює, відповідно, 8,4% від загальної кількості замовлених магістрів. Виникає питання, чи є достатнім такий відсоток відповідних фахівців для потреб цих міністерств та відомств?

Доцільно відзначити, що СБ України та Адміністрація Держприкордонслужби зовсім не увійшли до кола замовників. І, якщо на базі навчально-наукового інституту інформаційної безпеки Національної академії СБ України здійснюється підготовка фахівців для потреб відомства, зокрема за спеціальністю "Кібербезпека", то такої практики в Держприкордонслужбі немає. Натомість в її складі діє Центр кібербезпеки Головного центру зв'язку, автоматизації та захисту інформації, співробітники якого повинні бути справжніми фахівцями із кібербезпеки.

Аналізуючи державне замовлення фахівців із кібербезпеки протягом 2017 – 2019 рр., необхідно відзначити роль Міністерства освіти і науки України, яке є державним замовником у підготовці відповідних фахівців як для основних суб'єктів національної системи кібербезпеки, так і для приватних фірм та компаній. На думку деяких аналітиків, у подальші тридцять років галузь кібербезпеки буде динамічно розвиватися та збільшуватися, тож і попит на відповідних спеціалістів буде значним і тривалим. Міністерству освіти і науки України, з її значущим науково-освітнім потенціалом у галузі підготовки і використання таких кадрів, було б доцільно врахувати цей тренд при розробці

концепцій та стратегій розвитку, тим більше, що нині такий дефіцит існує на внутрішньому українському ринку.

Має велике значення й відповідне державне замовлення на організацію різноманітних семінарів, тренінгів, навчань із військовослужбовцями та особами начальницького складу основних суб'єктів національної системи кібербезпеки. Відповідно до положень Стратегії кібербезпеки України, вжиття заходів, спрямованих на її забезпечення, має проводитися на планових засадах. Нині в масштабах держави не існує механізму визначення потреби на підвищення кваліфікації фахівців із кібербезпеки з числа військовослужбовців та осіб начальницького складу.

На сьогодні Адміністрація Держспецзв'язку, Нацполіція, СБ України, Міноборони, ГШ ЗС України та розвідувальні органи України самостійно планують організацію підвищення кваліфікації фахівців із кібербезпеки, що загалом не сприяє розвитку системи підготовки кадрів у сфері кібербезпеки.

Не менш важливим питанням є проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури, що є вимогою ст. 8 Закону України "Про основні засади забезпечення кібербезпеки України". Така періодична атестація (переатестація) персоналу повинна забезпечити оцінювання професійного рівня, ділових та моральних якостей кожного фахівця з кібербезпеки, його відповідності посаді, визначення перспективи службового використання, створення резерву кандидатів для просування по службі тощо. Впровадження такого механізму оцінювання особового складу, залученого до сфери кібербезпеки, повинно було би стати потужним виховним важелем для керівників усіх рівнів основних суб'єктів національної системи кібербезпеки. Однак на сьогодні зазначене питання залишилося не вирішеним.

Окремої уваги потребує питання підготовки кваліфікованих кадрів для потреб основних суб'єктів національної системи кібербезпеки та всієї держави. Моніторинг наукових публікацій останніх років, присвячених питанням підготовки фахівців у сфері кібернетичної безпеки, дав змогу виявити, що освітня діяльність галузі "Інформаційні технології" не охоплює підготовку фахівців за такими напрямами, як: захист мовної інформації на об'єктах інформаційної діяльності, організаційне управління інформаційною безпекою та охорона державної таємниці.

Проте, згідно з переліком галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, що затверджений Постановою Кабінету Міністрів України "Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти" № 266 від 29.04.2015 р., в Україні готуються фахівці тільки за спеціальністю "Кібербезпека", що не може, з урахуванням згаданого вище, забезпечити державу всіма необхідними фахівцями для забезпечення захисту інформації, що обробляється в ІТ-системах та озвучується на об'єктах інформаційної діяльності [13].

Тому, для забезпечення держави у майбутньому фахівцями за необхідними напрямами вбачається внести зміни до вищезазначеного переліку шляхом доповнення галуззю знань "Безпека та захист інформації", до якої будуть належати спеціальності: "Безпека інформаційно-комунікаційних систем", "Системи технічного захисту інформації", "Кібербезпека", "Управління інформаційною безпекою".

Для забезпечення плідної роботи спеціалістів у системі національної кібербезпеки потрібно не тільки ретельно здійснювати набір кадрів, а й приділяти також увагу організації їх підготовки. Особливу увагу потрібно приділяти практичній складовій навчання. Для цього необхідно не лише проводити навчання особового складу силами закладів освіти, але і створювати навчальні центри з вивчення питань інформаційної безпеки, кібербезпеки, кіберзахисту та захисту інформації в кіберпросторі.

Безумовно, для того, щоб існуючі проблемні питання були не лише декларативними, а дійсно запрацювали у сфері забезпечення кібербезпеки, необхідно запровадити дієвий механізм контролю щодо їх своєчасного та належного виконання всіма суб'єктами забезпечення кібербезпеки України, насамперед Національним координаційним центром кібербезпеки.

На сьогодні в державі вже починається процес розроблення проєкту нової Стратегії кібербезпеки України на наступні 2021 – 2025 рр. Однак без здійснення відповідної оцінки та вирішення проблемних питань щодо стану реалізації існуючої стратегії така робота лише засвідчить поверхневий та формальний підхід до питань кібербезпеки та кіберзахисту. З огляду на це, проблематика організації професійної підготовки фахівців із кібербезпеки стає особливо актуальною та порушує питання про подальший її розвиток для потреб основних суб'єктів національної системи кібербезпеки.

Висновки і перспективи подальших розвідок. Розвиток інформаційного суспільства та впровадження новітніх інформаційних технологій в усіх сферах суспільного життя є одним із найважливіших напрямів державної політики.

Водночас проведене дослідження засвідчило про недостатню розробленість нормативно-правової бази щодо організації та проведення різноманітних навчань із питань інформаційної безпеки, кібербезпеки та захисту інформації в кіберпросторі, насамперед на державному рівні. Встановлено фрагментарність регулювання цього питання. З'ясовано, що загальним недоліком проаналізованої нормативно-правової бази є невиконання на практиці основними суб'єктами національної системи кібербезпеки деяких положень та вимог вищезазначених документів.

Враховуючи проаналізований стан підготовки та підвищення кваліфікації фахівців основних суб'єктів національної системи кібербезпеки, беручи до уваги деякі прогалини у законодавстві, вважаємо доцільним:

– запровадження у структурах основних суб'єктів національної системи кібербезпеки окремих підрозділів (секторів, відділів, управлінь), що будуть

опікуватися питаннями підготовки та підвищення кваліфікації особового складу з питань кібербезпеки;

– розроблення проєктів наказу Адміністрації Держспецзв'язку щодо організації та впровадження проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури, та міжвідомчого наказу стосовно запровадження механізму визначення потреби на підвищення кваліфікації фахівців із кібербезпеки з числа військовослужбовців та осіб начальницького складу;

– внесення на розгляд Уряду проєкту постанови Кабінету Міністрів України щодо внесення змін до Переліку галузей знань і спеціальностей, за якими здійснюватиметься підготовка здобувачів вищої освіти, затвердженого Постановою Кабінету Міністрів України № 266 від 29.04.2015 р., шляхом доповнення галуззю знань "Безпека та захист інформації";

– розглянути питання щодо організації та проведення конференцій, семінарів, форумів, засідань, круглих столів, тренінгів, навчань із питань інформаційної безпеки, кібербезпеки, кіберзахисту та захисту інформації в кіберпросторі для фахівців основних суб'єктів національної системи кібербезпеки на базі центрів підвищення кваліфікації з інформаційних технологій, роботу яких потрібно організувати за територіальним принципом.

Сформульовані в роботі пропозиції та висновки можуть бути використані в практичній діяльності основних суб'єктів національної системи кібербезпеки, які беруть безпосередню участь у підготовці фахівців галузі знань "Інформаційні технології" та організації протидії кіберзагрозам під час формування сталої інформаційної політики держави та нормативно-правової бази.

Список використаної літератури

1. Діордіца І. Стан підготовки фахівців у сфері кібербезпеки. URL : http://vjhr.sk/archive/2016_6/part_1/11.pdf (дата звернення: 04.01.2020).

2. Діордіца І. Освітні стандарти підготовки фахівців із кібербезпеки. URL : http://jurnaluljuridic.in.ua/archive/2017/1/12.pdf (дата звернення: 04.01.2020).

3. Мельник С. Концептуальні основи організації професійної підготовки майбутніх фахівців із кібербезпеки // Педагогічні науки: теорія, історія, інноваційні технології. 2016. № 10. С. 79—88.

4. Бурячок В. Л., Пархомей І. Р., Степанов М. М., Толубко В. Б. Проблемні питання та актуальні завдання підготовки фахівців з кібернетичної безпеки галузі знань "Інформаційні технології" // Сучасний захист інформації. 2016. № 2. С. 4—9.

5. Кібербезпека в умовах розгортання четвертої промислової революції (industry 4.0): виклики та можливості для України : аналіт. доп. Національного інституту стратегічних досліджень від 15.05.2019 р. URL : https://niss.gov.ua/doslidzhennya/analitichni-materiali/informaciyni-strategii/kiberbezpeka-v-umovakh-rozgortannya (дата звернення: 04.01.2020).

6. Про основні засади забезпечення кібербезпеки України : Закон України № 2163-VIII від 05.10.2017 р. URL : https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 04.01.2020).

7. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України" : Указ Президента України № 287/2015 від 26.05.2015 р. URL : https://zakon.rada.gov.ua/laws/show/287/2015 (дата звернення: 04.01.2020).

8. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" : Указ Президента України № 96/2016 від 15.03.2016 р. URL : https://zakon5.rada.gov.ua/laws/show/96/2016 (дата звернення: 04.01.2020).

9. Про Національний координаційний центр кібербезпеки : Указ Президента України № 242/2016 від 07.06.2016 р. URL : https://zakon.rada.gov.ua/laws/show/242/2016 (дата звернення: 04.01.2020).

10. Про затвердження плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України : Розпорядження Кабінету Міністрів України № 440-р від 24.06.2016 р. URL : https://zakon.rada.gov.ua/laws/show/440-2016-%D1%80 (дата звернення: 04.01.2020).

11. Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України : Розпорядження Кабінету Міністрів України № 155-р від 10.03.2017 р. URL : https://zakon.rada.gov.ua/laws/show/155-2017-%D1%80 (дата звернення: 04.01.2020).

12. Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України : Розпорядження Кабінету Міністрів України № 481-р від 11.07.2018 р. URL : https://zakon.rada.gov.ua/laws/show/481-2018-%D1%80 (дата звернення: 04.01.2020).

13. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти : Постанова Кабінету Міністрів України № 266 від 29.04.2015 р. URL : https://zakon.rada.gov.ua/laws/show/266-2015-%D0%BF (дата звернення: 04.01.2020).

Статтю подано: 17.01.2020 *Статтю схвалено: 03.03.2020*

Arsenovych Leonid Antonovych

deputy head – head of division at the HR Management Department of the Administration of the State Service for Special Communication and Information Protection of Ukraine, post-graduate student of the Information Policy and Digital Technology Department at the National Academy for Public Administration under the President of Ukraine

ORCID: 0000-0001-7081-2838

e-mail: arsen-leon@ukr.net

ORGANIZATION OF VOCATIONAL TRAINING OF CYBER SECURITY PROFESSIONALS BY MAIN SUBJECTS OF THE NATIONAL CYBER SECURITY SYSTEM: PRACTICAL ASPECT

Problem setting. In the context of digital world and information technology development, special focus is made on issues related to professional training of IT specialists, and primarily of cybersecurity specialists within the security and defense authorities of Ukraine.

Fundamental and advanced training as well as re-training of cybersecurity specialists are the challenges faced in safeguarding cybersecurity in Ukraine. In light of extensive reforms being implemented in all life areas of the Ukrainian society, proper training for

cybersecurity specialists of the security and defense authorities of Ukraine is getting especially relevant and requires special attention of the leaders of these security and defense authorities.

Recent research and publications analysis. The analysis has identified that principally the development, through effective reforms, of the system of fundamental and advanced training as well as re-training of people employed in the institutions committed to safeguarding the Ukrainian cybersecurity is one of the ways to implement the Cybersecurity Strategy of Ukraine and the Concept for the Development of the Security and Defense Sector of Ukraine.

At the same time, one should acknowledge that the issue of implementing the Cybersecurity Strategy of Ukraine and other regulations has been taken beyond the focus of comprehensive scientific research studies. In practice, this results in the understated importance of training for the personnel of the security and defense sector entities, which is one of the priorities and ways of safeguarding cybersecurity in Ukraine.

Highlighting previously unsettled parts of the general problem. The publication aims to outline the challenges related to professional training of cybersecurity specialists. To achieve the target, the following issues require being addressed: analysis of regulatory framework of professional training for cybersecurity specialists; study of issues related to procurement of training and training itself in the area of information security, cybersecurity, cyberprotection and data protection in cyberspace during 2016 – 2018 by the core Ukrainian security and defense sector entities; giving practical recommendations to government authorities on how to improve the system of professional training for cybersecurity specialists.

Paper main body. Now, training of qualified personnel remains the key component of self-sufficient operation of the country. The issue of professional training of cybersecurity specialists can be found incorporated in a number of regulations made and approved by the Verkhovna Rada of Ukraine, President of Ukraine and Cabinet of Ministers of Ukraine (Law of Ukraine "On Fundamentals of Safeguarding Cybersecurity of Ukraine"; Strategy of the National Security of Ukraine; Cybersecurity Strategy of Ukraine; Regulation on the National Coordination Center for Cybersecurity; and the Cabinet's decrees for the respective year that directly approve the Ukrainian Cybersecurity Strategy implementation measures).

The analysis in the publication shows that the major weaknesses of procuring the professional training of cybersecurity specialists by the Ukrainian security and defense sector entities are the lack:

– of dedicated divisions (sectors, units, subdivisions) within the ministries and departments being the entities of the security and defense sector of Ukraine, which would be in charge of the issues related to training, qualification and advanced training of personnel, and primarily the issues of cybersecurity, cyberprotection, information security and data protection in cyberspace;

– of procedure to identify the need for advanced training of cybersecurity specialists from among the military service personnel or the leaders;

– of mandatory regular certification (re-certification) of the personnel in charge of safeguarding the cybersecurity;

– of training centers dedicated to issues of information security, cybersecurity, cyberprotection and data protection in cyberspace.

Given the above, the challenges of procuring professional training for cybersecurity specialists are getting especially relevant and particularly require raising issues about further

development of such procurement to address the needs of the security and defense authorities of Ukraine.

Conclusions of the research and prospects for further studies. Development of the information-oriented society and implementation of the cutting-edge information technology in all life areas of the community and government authorities is one of the critical directions of the state policy.

Meanwhile, the research has shown the underworked nature of the regulatory framework of procurement and provision of various types of training in the area of information security, cybersecurity and data protection in cyberspace, and primarily at the government level. The research has also identified the fragmentary nature of regulating this issue. It has been discovered that the general weakness of the analyzed regulatory framework is the failure of practical fulfillment of most provisions and requirements incorporated in the above documents.

The conclusions and recommendations made during the work process can be used in practical activities of the government authorities that directly participate in training the "Information Technology" specialists and in combating cyberthreats in the process of developing the sustainable state information policy and the regulatory framework.

Key words: information security; information technology; cybersecurity; cyberprotection; professional training; Cybersecurity Strategy.

References

1. Diorditsa, I. (2016). *Stan pidhotovky fakhivtsiv u sferi kiberbezpeky*. URL : http://vjhr.sk/archive/2016_6/part_1/11.pdf [in Ukrainian].

2. Diorditsa, I. (2017). *Osvitni standarty pidhotovky fakhivtsiv iz kiberbezpeky*. URL : http://jurnaluljuridic.in.ua/archive/2017/1/12.pdf [in Ukrainian].

3. Melnyk, S. (2016). Kontseptualni osnovy orhanizatsii profesiinoi pidhotovky maibutnikh fakhivtsiv iz kiberbezpeky. *Pedagogical sciences: theory, history, innovative technologies*, Issue 10, pp. 79-88 [in Ukrainian].

4. Buriachok, V., Parkhomei, I. R., Stepanov, R. R., Tolubko, V. B. (2016). Problemni pytannia ta aktualni zavdannia pidhotovky fakhivtsiv z kibernetychnoi bezpeky haluzi znan "Informatsiini tekhnolohii". *Modern protection of information*, Issue 2, pp. 4-9 [in Ukrainian].

5. Kiberbezpeka v umovakh rozghortannia chetvertoi promyslovoi revoliutsii (industry 4.0): vyklyky ta mozhlyvosti dlia Ukrainy. (2019). URL : https://niss.gov.ua/doslidzhennya/analitichni-materiali/informaciyni-strategii/kiberbezpeka-v-umovakh-rozgortannya [in Ukrainian].

6. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy. № 2163-VIII. (2017) [in Ukrainian].

7. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 6 travnia 2015 roku "Pro Stratehiiu natsionalnoi bezpeky Ukrainy". № 287/2015. (2015) [in Ukrainian].

8. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku "Pro Stratehiiu kiberbezpeky Ukrainy". № 96/2016. (2016) [in Ukrainian].

9. Pro Natsionalnyi koordynatsiinyi tsentr kiberbezpeky. № 242/2016. (2016) [in Ukrainian].

10. Pro zatverdzhennia planu zakhodiv na 2016 rik z realizatsii Stratehii kiberbezpeky Ukrainy. № 440-r. (2016) [in Ukrainian].

11. Pro zatverdzhennia planu zakhodiv na 2017 rik z realizatsii Stratehii kiberbezpeky Ukrainy. № 155-r. (2017) [in Ukrainian].

12. Pro zatverdzhennia planu zakhodiv na 2018 rik z realizatsii Stratehii kiberbezpeky Ukrainy. № 481-r. (2018) [in Ukrainian].

13. Pro zatverdzhennia pereliku haluzei znan i spetsialnostei, za yakymy zdiisniuietsia pidhotovka zdobuvachiv vyshchoi osvity. № 266. (2015) [in Ukrainian].

Paper submitted: 17.01.2020 *Paper accepted: 03.03.2020*

Цитування: Арсенович Л. А. Організація професійної підготовки фахівців із кібербезпеки основними суб'єктами національної системи кібербезпеки: практичний аспект // Ефективність державного управління : зб. наук. пр. Вип. 1 (62) : у 2 ч. Ч. 1 / за заг. ред. чл.-кор. НАН України В. С. Загорського, доц. А. В. Ліпенцева. Львів : ЛРІДУ НАДУ, 2020. С. 91—105. (DOI: https://doi.org/10.33990/2070-4011.62.2020.205817).

Citation: Arsenovych, L. A. (2020). Organization of vocational training of cyber security professionals by main subjects of the national cyber security system: practical aspect : practical aspect. *Efficiency of Public Administration*, Issue 1 (62), pp. 91-105. (DOI: https://doi.org/10.33990/2070-4011.62.2020.205817).