

УДК 342.9

## СУЧАСНИЙ СТАН НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ПІДГОТОВКИ ФАХІВЦІВ ІЗ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Оксана ТОПЧІЙ,  
кандидат педагогічних наук

### АНОТАЦІЯ

У роботі проаналізовано нормативно-правову базу, що регулює питання підготовки, перепідготовки та підвищення кваліфікації фахівців із кібербезпеки в Україні; визначено основні напрями її вдосконалення.

**Ключові слова:** нормативно-правові акти, підготовка, перепідготовка, підвищення кваліфікації фахівців із кібербезпеки в Україні.

### THE CURRENT STATE OF THE LEGAL REGULATION OF THE TRAINING OF SPECIALISTS IN CYBERSECURITY IN UKRAINE

Oksana TOPCHII,  
Candidate of Pedagogical Sciences

In the article analysis normative-legal base, which regulates questions of training, retraining and improvement of professional skill of cybersecurity specialists in Ukraine; the main directions of its improvement are determined.

**Key words:** normative-legal acts, training, retraining and improvement of professional skill of cybersecurity specialists in Ukraine.

**Постановка проблеми.** Для захисту життєво важливих інтересів людини й громадянина, суспільства та держави, а також національних інтересів України в кіберпросторі є потреба у високопрофесійних кадрах, здатних ефективно виконувати поставлені перед ними завдання. Зважаючи на це, одним із пріоритетів державної політики у сфері кібербезпеки є підготовка кадрів і підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки за допомогою відповідної системи. Забезпечення ефективного функціонування такої системи передбачає, серед іншого, наявність нормативно-правової бази, яка наразі перебуває на етапі формування.

**Актуальність теми дослідження.** Таким чином, саме необхідність визначення основних напрямів удосконалення нормативно-правового регулювання підготовки фахівців із кібербезпеки в Україні й визначає актуальність цієї статті.

**Стан дослідження.** Проблематику підготовки кадрів в інформаційній сфері, міжнародний досвід організації навчального процесу, досягнення й пропозиції нормативно-правового регулювання у сфері кібербезпеки вивчали Р.О. Банк, О.А. Баранов, Ю.Г. Даник, М.І. Дімчогло, І.В. Діордіца, Д.В. Дубов, В.А. Залізник, Є.Ф. Збінський, Б.А. Кормич, В.А. Ліпкав, Ю.Є. Максименко, О.А. Мандзюк, П.Є. Матвієнко, С.В. Мельник, В.М. Панченко, В.Я. Політило, Л.І. Рудник, Л.В. Скрипник, К.Г. Татарникова, О.О. Тихомиров, О.В. Шепета й інші.

Однак ступінь дослідженості основних напрямів удосконалення нормативно-правового регулювання підготовки фахівців із кібербезпеки в Україні в контексті змін і доповнень, що були внесені до законодавства протягом останніх років, наразі залишається недостатнім.

**Мета й завдання статті.** Основними завданнями, розв'язання яких присвячена ця стаття, є такі: дослідити сучасний стан нормативно-правового регулювання підготовки фахівців із кібербезпеки в Україні; визначити перспективні напрями подальших розвідок із досліджуваних питань.

**Виклад основного матеріалу.** Серед основних чинників, що зумовлюють принципову важливість питання

підготовки та підвищення кваліфікації фахівців у галузі кібербезпеки, слід назвати транснаціональний характер інформаційного простору, зростання кількості злочинів у цій сфері та глобалізований характер кібернетичної безпеки. Вивчення наукового доробку вітчизняних і зарубіжних науковців і практиків свідчить, що професійна підготовка фахівців із кібербезпеки є однією зі складових частин національної безпеки, без якої є неможливим науково-технічний і соціально-економічний розвиток країни [1, с. 7].

Україна має значний потенціал у галузі підготовки фахівців із кібербезпеки. Бакалаврів і магістрів за спеціальністю «Кібербезпека» станом на вересень 2018 р. готують 53 вітчизняних ВНЗ (зокрема й при профільних відомствах – ДССЗЗІ, СБУ, МВС, МО України, розвідувальних органах тощо), а обсяги державного замовлення на цих фахівців останніми роками постійно зростають [2].

Проте експерти констатують також і наявність системних проблем у цій сфері [3]:

- відсутність належного рівня кваліфікації в підготовці сучасних фахівців із питань кібербезпеки й інформаційної безпеки в закладах освіти;
- низький рівень зарплатні професорсько-викладацького складу в інститутах і фінансування фахівців у державних компаніях;
- застарілу навчальну програму з підготовки фахівців із питань кібербезпеки й інформаційної безпеки;
- відсутність координації в системі освіти між замовниками кадрів і закладами освіти;
- відірваність фахівців з інформаційної та кібербезпеки від міжнародної системи стандартизації;
- брак наукових досліджень із проблем кібербезпеки.

У цих умовах особливої актуальності набуває положення, досить точно сформульоване в дослідженні О.В. Поступної, яка зазначає, що для успішного здійснення процесів модернізації освітньої сфери важливе значення має правове регулювання цієї сфери, яке стає дійсним інструментом розвитку вітчизняної освіти [4].

Питання підготовки, перепідготовки та підвищення кваліфікації фахівців із кібербезпеки в Україні регламенту-

ються масивом нормативно-правових документів, до якого входять як закони України, так і підзаконні акти. При цьому поняття «фахівець із кібербезпеки» ми розглядаємо в широкому розумінні, тобто до цієї категорії входять особи, які за родом своєї професійної діяльності можуть використовувати спеціальні знання для попередження потенційних загроз, викриття/розкриття, нейтралізації чи мінімізації наслідків протиправної поведінки правопорушників у комп'ютерному просторі [5, с. 201].

Умовно можна виділити кілька груп документів, що стосуються питань функціонування системи підготовки фахівців із кібербезпеки в Україні. Зокрема, це нормативно-правові акти щодо організації та координації навчання, а також визначення вимог до навчальних закладів для навчання фахівців із кібербезпеки.

Основні засади нормативно-правового регулювання *організації та координації навчання фахівців із кібербезпеки* визначені в Законі України «Про вищу освіту» [6]. Зокрема, згаданим Законом України встановлені основні правові, організаційні та фінансові засади функціонування системи вищої освіти; розкрито зміст і порядок реалізації права на вищу освіту в Україні; визначені рівні, ступені та кваліфікації вищої освіти; закріплені вимоги щодо стандартів освітньої діяльності та вищої освіти; розкриті засади управління у сфері вищої освіти та системи забезпечення якості вищої освіти; установлені вимоги до закладів вищої освіти та порядку управління ними. Окрему увагу в Законі приділено питанням доступу до вищої освіти, прийому, відрахування, переривання навчання, поновлення й переведення осіб, які навчаються в закладах вищої освіти, а також організації освітнього процесу [6].

Постановою Кабінету Міністрів України «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 29 квітня 2015 р. № 266 (зі змінами, внесеними згідно з Постановами Кабінету Міністрів України № 674 від 27 вересня 2016 р. і № 53 від 01 лютого 2017 р.) [7] визначено, що спеціальність «Кібербезпека» (код 125) входить до галузі знань «Інформаційні технології» та з 1 вересня 2015 р. є одною зі спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти в Україні.

Умови прийому на навчання до закладів вищої освіти України в 2018 р. регулюються Наказом Міністерства освіти й науки України від 13 жовтня 2017 р. № 1378 «Про затвердження деяких нормативно-правових актів з питань прийому на навчання до закладів вищої освіти» [8]. Цей Наказ зареєстрований відповідним чином у Міністерстві юстиції України, а отже, також входить до блоку загальнообов'язкових нормативно-правових документів із питань організації та координації навчання фахівців із кібербезпеки.

Серед нагальних проблем нормативно-правового регулювання організації та координації навчання фахівців із кібербезпеки сучасні вчені називають насамперед те, що за відсутності переліку професій, пов'язаних із забезпеченням кібернетичної безпеки, у державних стандартах України, нерозробленістю професіограм для цієї категорії фахівців вищі навчальні заклади здійснюють підготовку здобувачів вищої освіти без урахування комплексу всіх специфічних особливостей формування висококваліфікованого персоналу для подальшої роботи в життєво важливій сфері діяльності [9, с. 20].

**Вимоги до навчальних закладів, які здійснюють підготовку фахівців із кібербезпеки в Україні**, визначаються Постановами Кабінету Міністрів України від 30 грудня 2015 р. № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності» [10] і від 09 серпня 2001 р. № 978 «Про затвердження Положення про акредитацію вищих навчальних закладів і спеціальностей у вищих на-

вчальних закладах і вищих професійних училищах» [11]. Зазначеними документами врегульовані питання ліцензування освітньої діяльності, тобто встановлена спроможність закладу освіти провадити освітню діяльність відповідно до встановлених ліцензійними умовами вимог, а також питання акредитації, тобто державного визнання відповідності рівня підготовки (перепідготовки) фахівців державним вимогам до напряму підготовки, спеціальності та вищого навчального закладу, затвердженим МОН.

Так, Постановою Кабінету Міністрів України від 30 грудня 2015 р. № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності» [10] визначається таке:

- кадрові вимоги щодо забезпечення започаткування освітньої діяльності;
- кадрові вимоги щодо забезпечення провадження освітньої діяльності;
- технологічні вимоги щодо забезпечення започаткування та провадження освітньої діяльності;
- організаційні вимоги щодо забезпечення започаткування та провадження освітньої діяльності;
- перелік документів, що підтверджують відповідність закладу освіти вимогам щодо започаткування та провадження освітньої діяльності.

Також Постановою Кабінету Міністрів України від 09 серпня 2001 р. № 978 «Про затвердження Положення про акредитацію вищих навчальних закладів і спеціальностей у вищих навчальних закладах і вищих професійних училищах» [11] визначається таке:

- порядок проведення акредитації;
- права й обов'язки навчального закладу;
- фінансування проведення акредитації;
- порядок оскарження рішень Акредитаційної комісії.

Серед актуальних проблем нормативно-правового регулювання вимог до навчальних закладів, які здійснюють підготовку фахівців із кібербезпеки в Україні, у наукових колах частіше за все називають ту обставину, що попри наявність у низки вищих навчальних закладів ліцензій на підготовку бакалаврів і магістрів за спеціальністю 125 «Кібербезпека», методологічні й методичні засади стандартизації вказаної освіти потребують крос-наукового обґрунтування, а також суттєвого перегляду наявних підходів із метою забезпечення всіх потреб держави в цій галузі на сучасному рівні. Із позицій науки ця проблема розглядається здебільшого в контексті освітньої діяльності галузі знань «Інформаційні технології». У цих умовах більш широкий підхід дозволить комплексно підійти до вивчення проблеми, виокремити коло проблемних питань, без рішення яких сфера національної безпеки, реалізації прав і свобод громадян залишиться перед реальними, а не потенційними загрозами з боку світу кіберзлочинності [9, с. 21].

Окремої уваги заслуговує питання *нормативно-правового регулювання кваліфікаційних вимог до компетенції фахівців із кібербезпеки*.

Річ у тім, що сьогодні формулювання кваліфікаційних вимог до компетенцій фахівців із кібербезпеки знаходиться в стані розроблення. Як зазначає І.В. Діордіца, практиці підбору кадрів бракує науково обґрунтованих кваліфікаційних характеристик фахівців, без яких забезпечення безпеки в інформаційно-комунікативному просторі стає доволі проблематичним. Незважаючи на усвідомлення компетентними органами державної влади важливості підготовки фахівців із кібербезпеки, є чимало проблем у розробленні освітніх стандартів для цієї категорії здобувачів вищої освіти [9, с. 20].

Основними компетенціями фахівців із кібербезпеки, що мають знайти відображення в нормативно-правовій базі, найчастіше називають такі:

– здатність розуміти сутність і значення інформації в розвитку сучасного інформаційного суспільства, застосувати досягнення інформатики й обчислювальної техніки, проводити цілеспрямований пошук і збір інформації з відкритих, а також її добування з відносно відкритих і закритих електронних джерел;

– здатність виявляти ознаки стороннього кібернетичного впливу, а також моделювати можливі ситуації такого впливу та прогнозувати їх можливі наслідки;

– здатність організувати й підтримувати комплекс заходів щодо забезпечення інформаційної й кібербезпеки з урахуванням їхньої правової обґрунтованості, адміністративно-управлінської й технічної можливості реалізації й економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації;

– здатність протидіяти несанкціонованому проникненню протилежних сторін до власних ІТ-систем і мереж, забезпечити стійкість їх роботи, а також відновлення їх нормального функціонування після здійснення кібернападів;

– здатність організувати проведення атестації об'єкта на відповідність вимогам державних або корпоративних нормативних документів;

– здатність брати участь у розробленні підсистем управління інформаційною й кібербезпекою, здійснювати їх адміністрування й експлуатацію;

– здатність до проведення попереднього техніко-економічного аналізу й обґрунтування проектних рішень із забезпечення кібербезпеки;

– здатність оформлювати технічну документацію з урахуванням чинних нормативних і методичних документів у галузі інформаційної й кібербезпеки;

– здатність до програмної реалізації алгоритмів рішення типових завдань забезпечення інформаційної й кібербезпеки й до застосування програмних засобів системного, прикладного й спеціального призначення;

– здатність проводити аналіз інформаційної безпеки об'єктів і систем із використанням вітчизняних і закордонних стандартів;

– здатність формувати комплекс заходів (правила, процедури, практичні прийоми й ін.) для керування інформаційною й кібербезпекою тощо [12, с. 129–130].

Однак донині ці компетенції не знайшли свого закріплення в нормативно-правовій базі з питань підготовки фахівців із кібербезпеки.

*Отже, оскільки підготовка фахівців із кібербезпеки в Україні здійснюється у вищих навчальних закладах, то нормативно-правові документи, якими визначені вимоги до навчальних закладів, а також ті, якими врегульовується організація та координація навчання, є важливою складовою частиною нормативно-правової бази підготовки фахівців із кібербезпеки в Україні.*

При цьому в цілому ми приєднуємося до наявної наукової позиції, згідно з якою поняття «фахівець із кібербезпеки» не повинне обмежуватися лише групою осіб, які здобули вищу освіту за зазначеним фахом. Процес підготовки кадрів, підвищення їх кваліфікації в цьому напрямі з урахуванням усіх аспектів діяльності й сфер життя держави, зокрема й у галузі міжнародного співробітництва, має здійснюватися на інтеграційних засадах кореляції всіх складників кібернетичної безпеки [9, с. 20].

Для збереження належної конкурентоспроможності та професійного рівня фахівців із кібербезпеки необхідно постійно підвищувати свою кваліфікацію на засадах так званої концепції безперервної освіти (або «освіти протягом життя»). Можливі декілька варіантів роботи в цьому напрямі, серед яких – перепідготовка в рамках післядипломної освіти фахівців у споріднених із кібернетичною

безпекою спеціальностях, застосування нелінійної схеми підготовки фахівців, використання потенційних можливостей неформальної освіти для підвищення кваліфікації діючих фахівців через проведення тренінгів, семінарів, міжнародних стажувань тощо [13, с. 15].

Щодо такого наукового погляду, то маємо зауважити, що нормативно-правове регулювання підготовки фахівців із кібербезпеки в Україні здійснюється також окремими профільними документами з питань кібербезпеки.

У розрізі предмета нашого дослідження неможливо оминути увагою один із найважливіших негативних чинників, що знижує ефективність нормативно-правового регулювання підготовки фахівців із кібербезпеки в Україні. Маємо на увазі відсутність окремого законодавчого акта, який консолідував би всі елементи реалізації кібернетичної безпеки, зокрема й пов'язані з підготовкою фахівців діяльності цієї сфери.

Безперечно, у цьому напрямі робляться певні кроки. Так, восени 2016 р. був прийнятий Закон України «Про основні засади забезпечення кібербезпеки України», в якому визначені правові й організаційні основи забезпечення захисту життєво важливих інтересів людини й громадянина, суспільства та держави, національних інтересів України в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб і громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [14].

У ч. 1 ст. 3 згаданого Закону наведений перелік правових джерел, що становлять правову основу забезпечення кібербезпеки України. Окрім Конституції України, законів України щодо основ національної безпеки, засад внутрішньої й зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, та інших законів України, до цього переліку увійшли також Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України [14].

Дослідження змісту документів, які згідно із Законом України «Про основні засади забезпечення кібербезпеки України» [14] є правовою основою забезпечення кібербезпеки України, у розрізі предмета нашого дослідження дозволяє дійти деяких висновків.

Розроблення й реалізація освітніх заходів у сфері кібербезпеки, кібероборони та кіберзахисту визначені в якості одного з обов'язків суб'єктів забезпечення кібербезпеки відповідно до ч. 4 ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» [14]. Згідно зі ст. 10 указанного Закону України створення системи підготовки кадрів і підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки визначається як один із напрямів державно-приватної взаємодії у сфері кібербезпеки.

Слід зауважити, що питання державно-приватної взаємодії у сфері кібербезпеки останнім часом досить часто потрапляють у поле зору наукового товариства. Критична потреба в розвитку державно-приватної взаємодії в галузі кібербезпеки зумовлена в сучасному світі низкою причин, серед яких виокремлюються, насамперед, такі:

– активна приватизація деяких секторів критичної інфраструктури (що є не лише українським, але й глобальним трендом), унаслідок якої державні органи не можуть самостійно гарантувати повноту захисту критичної інформаційної інфраструктури;

– накопичення великої кількості електронних інформаційних ресурсів, які мають важливе значення для діяль-

ності як приватних власників, так і органів державного управління;

- залежність інфраструктури від інформаційно-телекомунікаційних систем і їхня вразливість;

- зростаюча конвергенція комп'ютерних мереж, унаслідок чого ураження однієї з інформаційно-комунікаційних систем може суттєво позначитися на функціонуванні інших;

- у підприємств малого та середнього бізнесу зазвичай бракує повноважень і ресурсів для повноцінного захисту власної інформаційної інфраструктури, тому вони зацікавлені в отриманні відповідних послуг від державних органів і/або від великих корпорацій [15, с. 56].

Саме тому різні форми державно-приватного партнерства розглядаються нині як один з основних інструментів побудови ефективних систем кіберзахисту й широко застосовуються в міжнародній практиці. Поряд із цим чинне профільне законодавство має низку суттєвих вад. У контексті проблематики державно-приватного партнерства основними з них експерти називають такі [13]:

- відповідні нормативні положення сформульовані дуже широко, при цьому спостерігається гострий дефіцит пов'язаних підзаконних актів, спрямованих на розвиток і конкретизацію таких положень. Насамперед це стосується галузевого регулювання захисту об'єктів кібербезпеки (з урахуванням специфіки різних секторів економіки), унормування інституту незалежних аудиторів і, зрештою, визначення правового змісту самого поняття «державно-приватна взаємодія»;

- суперечливими є норми, що визначають порядок упровадження аудиту інформаційної безпеки, установлюють вимоги до аудиторів інформаційної безпеки й визначають порядок їх атестації. Оскільки значна частина таких об'єктів знаходиться в недержавній власності, є вагомими підстави вважати, що визначені законодавством регулятивно-наглядні повноваження державних суб'єктів у цій галузі є надмірними й об'єктивно створюють передумови для зловживань, тиску на недержавний сектор (передусім бізнес) і створення корупційних схем;

- Законом «Про основні засади забезпечення кібербезпеки України» [14] встановлено, що порядок і методика здійснення аудиту кібербезпеки здійснюється на основі міжнародних стандартів, проте в його прикінцевих і перехідних положеннях немає жодної згадки про чинний Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», згідно зі ст. 7 якого «державні інформаційні ресурси чи інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтверженою відповідністю». Очевидно, що під дію цієї норми потрапляють практично всі об'єкти критичної інформаційної інфраструктури, значна кількість яких знаходиться в недержавному секторі (наприклад, в енергетиці, транспортній системі, телеком-індустрії, фармацевтиці тощо). Поряд із цим і сама Комплексна система захисту інформації, базована на українських стандартах, і вимога її обов'язкового застосування здебільшого піддається гострій критиці у вітчизняних експертних і бізнесових колах [13].

Отже, незважаючи на те, що саме освітній напрям часто називають одним із найбільш важливих і перспективних напрямів державно-приватної взаємодії у сфері кібербезпеки, а ст. 10 Закону України «Про основні засади забезпечення кібербезпеки України» [14] створення системи підготовки кадрів і підвищення цифрової грамотності громадян визнається як один із напрямів державно-приватної взаємодії у сфері кібербезпеки, питання інституційно-правового забезпечення повноцінної реалізації цієї норми залишається значною мірою невіршеним.

Ще одним документом, спрямованим на регулювання сфери кібербезпеки, є Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 р. № 96/2016 [16].

Згідно з п. 4.4 Стратегії [16], розвиток потенціалу сектора безпеки й оборони у сфері забезпечення кібербезпеки передбачатиме здійснення в установленому порядку заходів із розвитку системи підготовки кадрів для потреб органів сектора безпеки й оборони України та розвитку науково-виробничого потенціалу такої системи.

На виконання Стратегії кібербезпеки України [16] Кабінетом Міністрів України щорічно затверджується план заходів із реалізації Стратегії кібербезпеки України, до якого включаються також заходи щодо підготовки фахівців із кібербезпеки.

На 2018 р. такий план заходів затверджений розпорядженням Кабінету Міністрів України від 11 липня 2018 р. № 481-р [17]. Згідно з п. 16 згаданого плану, у межах розвитку системи підготовки кадрів у сфері кібербезпеки передбачене виконання таких заходів:

- підготовка фахівців тактичного й оперативно-тактичного рівня за напрямом «кібербезпека» (виконавець – Міноборони, Генеральний штаб Збройних Сил (за згодою); термін виконання – протягом року);

- підготовка, атестація, переатестація та підвищення кваліфікації фахівців у сфері кіберзахисту для потреб державних органів, військових формувань і правоохоронних органів (виконавець – Адміністрація Держспецзв'язку; термін виконання – протягом року).

Слід зауважити, що згадані пункти фактично без змін також входили в план заходів на 2017 р. із реалізації Стратегії кібербезпеки України, затверджений розпорядженням Кабінету Міністрів України від 10 березня 2017 р. № 155-р [18]. При цьому оскільки звітність за результатами виконання вищевказаного плану не доступна для широкого загалу, то оцінити результати виконання зазначених заходів фактично неможливо.

**Висновки.** Підсумовуючи отримані результати, можемо виділити дві відносно самостійні групи джерел нормативно-правового регулювання підготовки фахівців із кібербезпеки в Україні. Перша група – це нормативно-правові акти, якими врегульовані суспільні відносини у сфері вищої освіти в Україні. Друга група – це нормативно-правові акти, які регулюють суспільні відносини у сфері реалізації кібербезпекової політики в Україні. Саме на перетині цих двох груп перебуває нормативно-правове регулювання підготовки фахівців із кібербезпеки в Україні.

З урахуванням викладеного одним із перспективних напрямів подальших досліджень ми вважаємо вивчення досвіду нормативно-правового регулювання підготовки фахівців із кібербезпеки в зарубіжних країнах, що дозволить виявити конструктивні ідеї із цих питань задля їх творчої імплементації у вітчизняне законодавство.

#### Список використаної літератури:

1. Бистрова Б.В. Професійна підготовка бакалаврів з кібербезпеки у вищих навчальних закладах США: автореф. дис. на здобуття наук. ступеня канд. пед. наук : спец. 13.00.04 «теорія і методика професійної освіти». Київ, 2018. 23 с.
2. Довідник ВНЗ. Освіта.UA. URL: <https://osvita.ua/vnz/guide/search-17-0-0-42-43-0.html>.
3. Річний звіт VIII Українського форуму з управління Інтернетом. URL: [http://igf-ua.org/wp-content/uploads/2017/11/Ukrainian-IGF-UA\\_2017\\_Annual\\_Report\\_UKR.docx](http://igf-ua.org/wp-content/uploads/2017/11/Ukrainian-IGF-UA_2017_Annual_Report_UKR.docx).
4. Поступна О.В. Нормативно-правове забезпечення вищої освіти в Україні в контексті європейської інтеграції. Державне будівництво: електрон. вид. ХарПІ НАДУ. 2007. № 2. URL: <http://www.kbuapa.kharkov.ua>.

5. Діордіца І.В. Напрями підготовки та підвищення кваліфікації фахівців із кібербезпеки. Підприємництво, господарство і право. 2017. № 3. С. 199–203.

6. Про вищу освіту: Закон України від 1 липня 2014 р. Голос України. 2014. № 148.

7. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти : постанова Кабінету Міністрів України від 29 квітня 2015 № 266. Урядовий кур'єр. 2015. №102.

8. Про затвердження деяких нормативно-правових актів з питань прийому на навчання до закладів вищої освіти: Наказ Міністерства освіти і науки України від 13 жовтня 2017 р. № 1378, зареєстрований в Міністерстві юстиції України 14 листопада 2017 р. за № 1397/31265. Офіційний вісник України. 2017. № 97.

9. Діордіца І.В. Адміністративно-правове регулювання кібербезпеки України: автореф. дис. на здобуття наук. ступеня доктора юридичних наук: спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». Запоріжжя, 2018. 38 с.

10. Про затвердження Ліцензійних умов провадження освітньої діяльності: Постанова Кабінету Міністрів України від 30 грудня 2015 р. № 1187. Урядовий кур'єр. 2016. № 26.

11. Про затвердження Положення про акредитацію вищих навчальних закладів і спеціальностей у вищих навчальних закладах та вищих професійних училищах: Постанова Кабінету Міністрів України від 09 серпня 2001 р. № 978. Офіційний вісник України. 2001. № 32.

12. Бурячок В.Л., Богущ В.М. Рекомендації щодо розробки та запровадження профілю навчання «Кібернетична безпека» в Україні. Український науковий журнал інформаційної безпеки. 2014. № 20. С. 126–131.

13. Гнатюк С.Л. Актуальні питання розвитку державно-приватної взаємодії у сфері забезпечення кібербезпеки в Україні. Аналітична записка. Національний інститут стратегічних досліджень. URL: <http://www.niss.gov.ua/articles/2853/>.

14. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. Голос України. 2017. № 208.

15. Марушак А.І., Панченко В.М. Взаємодія державного та приватного секторів у сфері кібернетичної безпеки: іноземний досвід та перспективи для України. Інформаційна безпека, людина суспільство держава. 2014. № 3(16). С. 56–63.

16. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 № 96/2016. Офіційний вісник України. 2016. № 23.

17. Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України: розпорядження Кабінету Міністрів України від 11 липня 2018 р. № 481-р. Офіційний портал Верховної Ради України. URL: [www.rada.gov.ua](http://www.rada.gov.ua).

18. Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України: розпорядження Кабінету Міністрів України від 10 березня 2017 р. № 155-р. Офіційний портал Верховної Ради України. URL: [www.rada.gov.ua](http://www.rada.gov.ua).

#### ІНФОРМАЦІЯ ПРО АВТОРА

**Топчій Оксана Василівна** – кандидат педагогічних наук

#### INFORMATION ABOUT THE AUTHOR

**Topchii Oksana Vasylivna** – Candidate of Pedagogical Sciences