

## Правові й організаційні засади формування фахівців із кібербезпеки

### Legal and organizational bases of formation of cybersecurity specialists

Ігор Діордіца

#### Ключові слова:

кібербезпека, правові та організаційні засади, підготовка кадрів, формування фахівців.

#### Key words:

cybersecurity, legal and organizational framework, training, formation of professionals.

**Постановка проблеми.** Надскладні завдання, що постають перед державою на шляху захисту своїх інституцій, суспільства, громадян від злочинних посягань на їхні права, свободи в інформаційно-комунікативному просторі, потребують комплексного підходу до роботи з фахівцями, які у своїй професійній діяльності покликані забезпечувати кібернетичну безпеку. Цей підхід повинен мати всебічне наукове обґрунтування.

**Стан дослідження проблеми.** Формування фахівців є одним із головних завдань щодо поповнення ринку праці кваліфікованими професіоналами, спроможними виконувати на сучасному рівні покладені на них функції. Тому подібний аспект не може залишатися поза увагою науковців. Здебільшого ця проблема висвітлюється в наукових працях із педагогіки, зокрема йдеться про формування суб'єктності (С. Пелипчук), професійних здібностей (А. Клочко), професійних навичок (В. Єлов, В. Монастирський), професійно значущих якостей (В. Савіщенко), професійної культури (І. Михайліченко, М. Подберезький, В. Райко) майбутніх спеціалістів. Психологічні засади формування фахівця як суб'єкта правничої діяльності досліджувалися Н. Євдокимовою. Є низка публікацій із проблем підготовки кадрів із кібербезпеки в галузі знань «Інформаційні технології» (В. Бурячок, Ю. Даник, С. Демедюк, В. Марков, А. Міночкін, Ю. Супрунов та ін.).

Окремо варто виділити маститий доробок Інституту стратегічних комунікацій Глобальної організації союзницького лідерства, зокрема наукової школи доктора юридичних наук В. Ліпкана (В. Баскаков, Р. Банк, М. Дімчогло, В. Залізник, Є. Збінський, О. Климентьев, В. Кобринський, О. Кушнір, Д. Лобов, В. Майоров, Ю. Максименко, О. Мандзюк, П. Матвієнко, М. Микитенко, Д. Перов, В. Політило, С. Правдюк, Л. Рудник, О. Стоєцький, К. Татарникова, А. Тунік, К. Череповський, О. Шепета й ін.). У їхніх роботах закладено суттєвий фундамент для формування таких, що відповідають сучасним тенденціям розвитку, соціальних систем правових та організаційних засад формування фахівців із кібербезпеки<sup>1</sup>.

Разом із тим питання щодо правових та організаційних засад формування фахівців із кібербезпеки не було окремим предметом наукового дослідження. Розв'язання цієї проблеми дасть змогу в майбутньому вдосконалити нормативну регламентацію процесів підготовки професіоналів у зазначеній галузі.

**Мета статті** полягає в аналізі чинних правових та організаційних засад формування фахівців із кібербезпеки.

Для досягнення поставленої мети необхідно виконати низку завдань:

1. Установити сутність ключового поняття «формування фахівців із кібербезпеки».
2. Визначити коло нормативно-правових актів, якими регламентується цей процес.
3. Окреслити організаційні засади зазначеного процесу.
4. Виявити шляхи вдосконалення діяльності в напрямі, що досліджується.

<sup>1</sup> Ліпкан В.А. Адміністративно-правовий режим інформації з обмеженим доступом в Україні : [монографія] / В.А. Ліпкан, В.Ю. Баскаков ; за заг. ред. В.А. Ліпкана. – К. : О.С. Ліпкан, 2013. – 344 с.

**Виклад основного матеріалу.** Одне з ключових понять теми статті – формування фахівця, по суті, є категорією низки гуманітарних наук. У підготовці кадрів, поповненні ринку праці висококваліфікованими кадрами воно посідає чільне місце поряд із такими категоріями, як підготовка, освіта, навчання, розвиток, виховання тощо.

І. Подласий зазначає, що, незважаючи на широке застосування, поняття «формування» ще не є усталеною категорією, й пропонує розуміти під ним «процес становлення людини як соціальної істоти під впливом усіх без винятку чинників – екологічних, соціальних, економічних, ідеологічних, психологічних тощо»<sup>2</sup>. Консолідуєчись із тим, що процес формування відбувається під впливом комплексу чинників, ми, тим не менше, не розділяємо позиції вченого щодо тлумачення цієї категорії через становлення людини як соціальної істоти, оскільки подібне бачення швидше відповідає семантиці поняття «соціалізація особистості», а не формування. Для нас більш прийнятним є варіант інтерпретації ключового поняття, запропонований Г. Ложки, який розглядає формування як результат активних форм впливу зовнішніх і внутрішніх факторів на процес розвитку особистості й професіонала<sup>3</sup>.

На думку Н. Євдокимової, формування суб'єкта професійної діяльності відбувається на стадії особистісної суб'єктності (за В. Селівановим), для якої характерні розвиток базових соціогенних потенцій, розвиток психічних функцій, досягнення акме психічної активності та внутрішньої визначеності, цільності<sup>4</sup>.

Отже, на цьому етапі є всі підстави розмежувати поняття підготовки й формування фахівця. Останнє є набагато ширшим, оскільки, окрім власне освітньо-інформаційних навчальних функцій, включає до свого семантичного поля розвиток і виховання особистості, прищеплення їй корпоративної професійної культури, створення умов для того, щоб надалі фахівець міг працювати нешаблонно, відповідально, мав соціально бажану систему переконань. Для такої категорії, як фахівець із кібербезпеки, це є вкрай важливим з урахуванням того, щоб надані в процесі навчання компетенції надалі не обернулися проти самого суспільства, щоб той, кого готували для запобігання правопорушенням у кібернетичному просторі, сам не став на злочинний шлях.

Конкретизуючи розуміння поняття «формування фахівця з кібербезпеки», ми вбачаємо, що цей процес є безперервним, і розглядаємо його як багатомірну категорію, яка включає до себе:

- формування фундаментальних світоглядних, гуманітарних і технічних професійно спрямованих компетентностей у сфері забезпечення кібернетичної безпеки в парадигмі правових норм, готовності особистості до постійного оновлення знань у зв'язку зі стрімким ускладненням інформаційних технологій і швидкою зміною тактики дій кіберзлочинців;
- формування суб'єктності професіонала в галузі кібербезпеки;
- формування стратегічного мислення фахівця, здатності працювати на випередження, прогнозувати можливі кібернетичні загрози;
- формування професійно значущих якостей особистості фахівця з кібербезпеки, зокрема розвитку важливих для професії здібностей особистості; прищеплення корпоративної кібербезпекової культури, системи соціально благочинних поглядів і переконань.

На відміну від традиційного навчання, процеси формування відбуваються не тільки в освітньому середовищі вищого навчального закладу, а й у колективах, де здобувачі вищої освіти проходять практики і стажування, під час спілкування з досвідченими фахівцями в галузі кібербезпеки, сприйняття, аналізу, інтерпретації інформації, що отримується майбутнім професіоналом у неформальних спільнотах, у медіа-просторі, в засобах масової інформації тощо.

У цьому зв'язку доречно процитувати висловлювання одного з фахівців ФБР США, наведене у відкритій публікації: "You don't make a cyber agent by sending them to training,.. It begins when they are very little,

<sup>2</sup> Подласый И.П. Педагогика. Новый курс : [учебник для студ. пед. вузов] : в 2 кн. / И.П. Подласый. – М. : Гуманит. изд. центр ВЛАДОС, 2000. – Кн. 1 : Общие основы. Процесс обучения. – 2000. – 176 с.

<sup>3</sup> Ложки Г.В. Психологические основы профессионализации личности в особых условиях деятельности / Г.В. Ложки // Актуальні проблеми становлення особистості професіонала в ризиконебезпечних професіях : матеріали Міжрегіон. наук. семінару (Київ, 25 берез. 2010 р.) / Мін-во оборони України, Національний університет оборони України. – К. : НУОУ, 2010. – С. 189–192.

<sup>4</sup> Євдокимова Н.О. Концептуальні підходи до формування майбутнього фахівця як суб'єкта правничої діяльності / Н.О. Євдокимова // Проблеми сучасної психології. – 2014. – Вип. 24. – С. 280–300.

it's a hobby to them, they grew up living and breathing technology"<sup>5</sup>. Тобто йдеться про те, що неможливо зробити кіберагента, посилаючи його на навчання. Усе починається змалечку, це має бути хобі для них; вони вирости, живучи й дихаючи технологіями.

Виходячи з наведеного, доходимо думки, що за державницького підходу варто було б запровадити практику, за якої формування фахівця з кібербезпеки починалося не зі студентської лави, а через пошук і супроводження вишами, майбутніми працедавцями талановитих дітей і молоді ще в період їх навчання в загальноосвітній середній школі, спеціалізованому ліцеї, в будинках дитячої творчості.

Отже, перед нами постає завдання встановити, як саме правові та організаційні засади детермінують процес становлення й розвитку майбутнього фахівця з кібербезпеки.

Безумовно, ми складаємо собі звіт у тому, що процес нормативно-правової регламентації формування фахівця з кібербезпеки є опосередкованим, оскільки закони й підзаконні акти України спрямовані на діяльність усіх вищих навчальних закладів, а не тільки тих, які здійснюють підготовку зазначених фахівців. Це означає, що, з одного боку, загальною правовою основою підготовки фахівця з кібербезпеки, як і будь-якого іншого здобувача вищої освіти, є Закони України «Про освіту», «Про вищу освіту», а з іншого боку, низка нормативно-правових актів, у тому числі міжнародних, що регламентують діяльність уповноважених суб'єктів у сфері транснаціональної, національної, інформаційної та кібернетичної безпеки.

Отже, згідно із Законом України «Про вищу освіту», підготовка фахівців із кібербезпеки, як і всіх інших здобувачів вищої освіти, передбачає ступеневість: молодший бакалавр, бакалавр, магістр, доктор філософії, доктор наук.

Не можна не помітити того, що на практиці, відповідно до державного замовлення й популярності спеціальності «кібербезпека» серед здобувачів вищої освіти, які навчаються за кошти фізичних осіб на контрактній основі, затребуваними є лише ступені бакалавра й магістра. На рівні молодших бакалаврів подібна підготовка практично не здійснюється. Разом із тим із позицій психофізіології саме цей віковий період, що умовно збігається з віком осіб, які готуються стати молодшими бакалаврами, є найбільш сприятливим для формування особистості, її якостей як професіонала.

Принагідно зауважимо, що контент-аналіз текстів правових актів, якими регулюються процеси освітньої діяльності (Закони України «Про освіту», «Про вищу освіту», «Про професійний розвиток працівників»), боротьби з кіберзлочинністю (проект Закону України «Про основні засади забезпечення кібербезпеки України», Укази Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про стратегію кібербезпеки України» від 15.03.2016 № 96/2016 і «Про національний координаційний центр з кібербезпеки» від 07.06.2016 № 242/2016), дав змогу встановити високу частотність ужитку, майже на рівні кліше, термінологічного сполучення «підготовка кадрів» на тлі майже повної відсутності сполуки «формування фахівців». І це не просто питання юридичної техніки. Це своєрідний концепт, за яким стоїть недооцінка комплексного підходу роботи з кадрами.

Загалом на рівні нормативно-правового регулювання діяльності з формування фахівців із кібербезпеки зафіксована доволі парадоксальна ситуація.

Ухвалення 29 квітня 2015 р. Кабінетом Міністрів України Постанови № 266, якою затверджується перелік галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти<sup>6</sup>, ознаменувалося запровадженням нової спеціальності за шифром 125 «Кібербезпека» в межах галузі «Інформаційні технології». Це створило передумови для ліцензування низки вишів для підготовки фахівців за цією спеціальністю. Одразу зазначимо, що виокремлення кібернетичної безпеки як окремої спеціальності стало суттєвим проривом для розв'язання стратегічних і тактичних завдань держави, що постають перед нею в період ускладнення ситуації в інформаційно-комунікативному просторі. Водночас подібний крок суттєво обмежив коло офіційно визнаних фахівців із кібербезпеки, залишивши поза його межами керівників і професіоналів сектору безпеки й оборони, банківського сектору, медійної сфери, які працюють у цій галузі за суміжним фахом.

<sup>5</sup> Kristina Davis. Why Cybercrime is So Hard to Investigate [Електронний ресурс]. – Режим доступу : <http://www.crime-research.org/articles/4002/>.

<sup>6</sup> Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти : Постанова Кабінету Міністрів України від 29 квітня 2015 р. № 266 (зі змінами, внесеними згідно з Постановою Кабінету Міністрів України від 27 вересня 2016 р. № 674) [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/266-2015-%D0%BF>.

Окремого коментаря потребує норма Закону України «Про вищу освіту», згідно з якою скасована лінійна схема підготовки фахівців, що дає можливість здобувачам освіти продовжувати навчання на більш високому ступені не тільки за іншою спеціальністю, а й за іншою галуззю знань<sup>7</sup>. Можливо, на думку фахівців із педагогіки вищої школи, подібне й не суперечить теорії навчання (хоча це ще треба довести), проте, як на наш розсуд, зазначена правова новела стосовно фахівців із кібернетичної безпеки є такою, що протистоїть інтересам суспільства. Обґрунтуємо. Законодавцем до уваги береться лише навчальний процес, опанування навчальної інформації згідно з освітньо-професійними програмами. У подібній ситуації виходить, що формування фахівця з кібербезпеки як цілісний безперервний процес, який є довготривалим і охоплює періоди становлення й розвитку особистості, виноситься за дужки. До уваги не береться той факт, що високоосвічений знавець у галузі інформаційних технологій, який не сформований як високоморальний професіонал із особливим типом мислення, корпоративною культурою, соціально спрямованою системою поглядів і переконань, може стати загрозою не тільки для українського суспільства, а й для світової спільноти загалом. Якщо в інших професіях формування фахівця здебільшого є педагогічною, частково економічною складовою, то стосовно фахівця з кібербезпеки процес його формування як особистості й професіонала необхідно розглядати в контексті глобальної та державної безпеки.

Неоднозначність ситуації, що склалася у сфері підготовки досліджуваної категорії фахівців із позицій її нормативної регламентації, виникає й через те, що, згідно з Національними класифікаторами, подібний вид діяльності та відповідні професії в Україні не передбачені.

Наприклад, у Класифікації видів економічної діяльності під шифром J міститься секція «Інформація та телекомунікації», де серед інших виділяється розділ 62 «Комп'ютерне програмування, консультування та пов'язана з ним діяльність». Зазначено, що цей розділ включає такі види експертної діяльності, як «написання, модифікування, тестування та забезпечення технічної підтримки програмного забезпечення; а також планування та розроблення комп'ютерних систем, які поєднують комплектуюче устаткування, програмне забезпечення та комунікаційні технології; місцеве керування та діяльність комп'ютерних систем клієнтів, а також оброблення даних та інші професійні та технічні види діяльності»<sup>8</sup>. Принагідно зазначимо стилістичну й граматичну неузгодженість тексту. У контексті ж питання, яке вивчається, можна припустити, що, вочевидь, кібернетична безпека потрапила до «інших професійних та технічних видів діяльності».

Пошуки в розділі 84 «Державне управління й оборона, обов'язкове соціальне страхування», де є класи 84.2 «Діяльність у сфері оборони», 84.3 «Діяльність у сфері юстиції і правосуддя», до яких могла б потрапити кібербезпека, також залишилися безплідними.

За логікою, раз немає певного виду економічної діяльності, то немає й відповідних йому професій. Звернення до Класифікатора професій – 2010<sup>9</sup> підтвердило нашу гіпотезу. Дійсно, ані серед категорії професіоналів, ані серед фахівців, ані серед технічних службовців нам не вдалося знайти прямої згадки про професії фахівців із кібербезпеки.

Незважаючи на те що на теперішній час з'явилося 87 томів Довідника кваліфікаційних характеристик професій працівників, серед них не знайшлося місця для опису еталонних індикаторів щодо осіб, які покликані виконувати функції із забезпечення кібернетичної безпеки держави, окремих закладів, установ, підприємств, організацій, у тому числі приватних.

У такий спосіб виявляється певна юридична суперечність: Кабінет Міністрів України запроваджує спеціальність «кібербезпека», щорічно робить державне замовлення на підготовку бакалаврів і магістрів за фахом, який не передбачений державними стандартами України у сфері видів економічної діяльності та професій.

Тож з'являються підстави припустити, що сьогодні немає й державно визнаних професіограм для фахівців із кібербезпеки, які б містили деталізований опис специфіки професійної діяльності, вимоги для осіб, які обіймають посади керівників, професіоналів і технічних працівників, професійно важливі якості особистості фахівця, психограми, критерії професійного відбору й особливості формування майбутнього спеціаліста. За відсутності професіограм освітньо-кваліфікаційні характеристики та освітньо-професійні

<sup>7</sup> Про вищу освіту : Закон України від 01.07.2014 (редакція від 30.11.2016) [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/1556-18>

<sup>8</sup> Класифікація видів економічної діяльності – 2010 [Електронний ресурс]. – Режим доступу : <http://dovidnyk.in.ua/directories/2010kved>

<sup>9</sup> Класифікатор професій ДК 003-2010 [Електронний ресурс]. – Режим доступу : <http://dovidnyk.in.ua/directories/profesii>.

програми стають безсистемними, необґрунтованими. Це, у свою чергу, не може не впливати на якість підготовки кадрів.

Подібна неузгодженість практично нівелює організаційні засади формування фахівців із кібербезпеки. Вищі навчальні заклади, які отримали ліцензії на освітню діяльність за сто двадцять п'ятою спеціальністю, фактично позбавлені орієнтирів щодо кінцевого результату діяльності, а тому проєктують усе на власний розсуд. Навіть в умовах децентралізації управління вищою освітою подібна ситуація не може розглядатися як сприятлива для задоволення державних потреб у фахівцях досліджуваного профілю.

Аналіз організаційних засад освітнього процесу в низці вищих навчальних закладів, що здійснюють підготовку фахівців за спеціальністю «кібербезпека», дав змогу встановити, що здебільшого здобувачів освіти готують до виконання функцій, пов'язаних із роботою з комп'ютерними програмами й обладнанням. Із поля зору укладачів освітніх стандартів на рівні вишів узагалі випадають або лише фрагментарно висвітлюються питання нормативно-правового забезпечення боротьби з кіберзлочинністю, з правопорушеннями у сфері інформаційного права, міжнародних стандартів діяльності у сфері кібернетичної діяльності. Студенти фактично не готуються до реалізації організаційно-управлінських, контрольних-аналітичних, прогностичних функцій. Подібна «технологізація» освіти в кінцевому підсумку стає чинником, який негативно впливає на формування фахівців із кібербезпеки, що надалі може перерости в серйозні проблеми для суспільства загалом.

**Висновки.** За результатами дослідження теми вдалося конкретизувати сутність поняття «формування фахівців із кібербезпеки», виявити правові та організаційні засади цього процесу. Установлено, що за відсутності переліку професій, пов'язаних із забезпеченням кібернетичної безпеки, у державних стандартах України, нерозробленості 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.

## Анотація

Стаття є результатом аналізу чинних правових та організаційних засад формування фахівців із кібербезпеки. Установлено сутність ключового поняття. Проведено порівняння категорій «підготовка кадрів» і «формування фахівців» із кібербезпеки. Визначено коло нормативно-правових актів, якими регламентуються зазначені процеси. Окреслено їх організаційні засади. Виявлено окремі аспекти, що потребують суттєвого переосмислення або доопрацювання, а також шляхи вдосконалення нормотворчості, практики діяльності вищих навчальних закладів, державних і недержавних інституцій, які є роботодавцями для фахівців із кібербезпеки.

## Summary

The article is the result of an analysis of existing legal and organizational bases of formation of cybersecurity specialists. The study begins with the establishment of the essence of the key concepts. The author concludes that the concept of "the formation of a specialist in cybersecurity" wider and deeper than the concept of "professional training on cyber security". The term "professional formation" includes within its semantic field of not only education, but also personal development, introduction to professional corporate culture, to create conditions for creativity, positive social attitudes. The author points out that the formation of a specialist in cybersecurity is not only in the educational environment, but also in communicating with professionals in informal communities, in the analysis of information from the media space. However, a content analysis of the texts of legislative acts (the Law of Ukraine "On Education", "On Higher Education", "On the professional development of workers"), the President of Ukraine decrees revealed that the concept of "the formation of a specialist" practically does not occur, and the notion of "personnel training" was a kind of cliché. The author's concept is that the formation of a specialist in cybersecurity consists of the formation of the fundamental, humanitarian and technical competence, the formation of subjectivity, the formation of strategic thinking and a global computer culture. All this should be reflected in the legal acts regulating the training of specialists in cybersecurity.

**Використана література:**

1. Ліпкан В.А. Адміністративно-правовий режим інформації з обмеженим доступом в Україні : [монографія] / В.А. Ліпкан, В.Ю. Баскаков ; за заг. ред. В.А. Ліпкана. – К. : О.С. Ліпкан, 2013. – 344 с.
2. Ліпкан В.А. Інкорпорація інформаційного законодавства України : [монографія] / В.А. Ліпкан, К.П. Череповський ; за заг. ред. В.А. Ліпкана. – К. : О.С. Ліпкан, 2014. – 408 с.
3. Ліпкан В.А. Консолідація інформаційного законодавства України : [монографія] / В.А. Ліпкан, М.І. Дімчогло ; за заг. ред. В.А. Ліпкана. – К. : О.С. Ліпкан, 2014. – 416 с.
4. Ліпкан В.А. Правовий режим податкової інформації в Україні : [монографія] / В.А. Ліпкан, О.В. Шепета, О.А. Мандзюк ; за заг. ред. В.А. Ліпкана. – К. : О.С. Ліпкан, 2015. – 440 с.
5. Ліпкан В.А. Систематизація інформаційного законодавства України : [монографія] / В.А. Ліпкан, В.А. Залізник ; за заг. ред. В.А. Ліпкана. – К. : О.С. Ліпкан, 2012. – 304 с.
6. Ліпкан В.А. Стратегічні комунікації : [словник] / В.А. Ліпкан, Т.В. Попова ; за заг. ред. доктора юридичних наук В.А. Ліпкана. – К. : ФОП Ліпкан О.С., 2016. – 416 с.
7. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції : [навчальний посібник] / В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський. – К. : КНТ, 2006. – 280 с.
8. Ліпкан В.А. Правові засади розвитку інформаційного суспільства в Україні : [монографія] / В.А. Ліпкан, І.М. Сопілко, В.О. Кір'ян ; за заг. ред. В.А. Ліпкана. – К. : ФОП О.С. Ліпкан, 2015. – 664 с.
9. Мандзюк О.А. Правове регулювання аналітичної діяльності в Україні : [монографія] / О.А. Мандзюк, М.Г. Сабіна. – К. : Дорадо-Друк, 2016. – 312 с.
10. Рудник Л.І. Право на доступ до інформації : дис. ... канд. юрид. наук : спец. 12.00.07 / Л.І. Рудник ; Національний університет біоресурсів і природокористування України. – К., 2015. – 247 с.
11. Подласый И.П. Педагогика. Новый курс : [учебник для студ. пед. вузов] : в 2 кн. / И.П. Подласый. – М. : Гуманит. изд. центр ВЛАДОС, 2000. – Кн. 1 : Общие основы. Процесс обучения. – 2000. – 176 с.
12. Ложки Г.В. Психологические основы профессионализации личности в особых условиях деятельности / Г.В. Ложки // Актуальні проблеми становлення особистості професіонала в ризиконебезпечних професіях : матеріали Міжрегіон. наук. семінару (Київ, 25 берез. 2010 р.) / Мін-во оборони України, Національний університет оборони України. – К. : НУОУ, 2010. – С. 189–192.
13. Євдокимова Н.О. Концептуальні підходи до формування майбутнього фахівця як суб'єкта правничої діяльності / Н.О. Євдокимова // Проблеми сучасної психології. – 2014. – Вип. 24. – С. 280–300.
14. Kristina Davis. Why Cybercrime is So Hard to Investigate [Електронний ресурс]. – Режим доступу : <http://www.crimere-search.org/articles/4002/>.
15. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти : Постанова Кабінету Міністрів України від 29 квітня 2015 р. № 266 (зі змінами, внесеними згідно з Постановою Кабінету Міністрів України від 27 вересня 2016 р. № 674) [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/266-2015-%D0%BF>.
16. Про вищу освіту : Закон України від 01.07.2014 (редакція від 30.11.2016) [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/1556-18>
17. Класифікація видів економічної діяльності – 2010 [Електронний ресурс]. – Режим доступу : <http://dovidnyk.in.ua/directories/2010kved>
18. Класифікатор професій ДК 003-2010 [Електронний ресурс]. – Режим доступу : <http://dovidnyk.in.ua/directories/profesii>.

**Ігор Діордіца,**

кандидат юридичних наук, доцент,  
голова Інституту адміністративного правосуддя  
Глобальної організації союзницького лідерства