# ПЕДАГОГІЧНІ НАУКИ

DOI: https://doi.org/10.31392/NZ-npu-145.2019.01
УДК 378.22 (410)

***Брайко Б. В.***

## УДОСКОНАЛЕННЯ ПРОФЕСІЙНОЇ ПІДГОТОВКИ МАГІСТРІВ З КІБЕРБЕЗПЕКИ В УМОВАХ ЄВРОІНТЕГРАЦІЙНИХ ПРОЦЕСІВ

*Стаття присвячена одній з актуальних проблем підготовки фахівців з кібербезпеки – реформуванню та модернізації системи ІТ-освіти на рівні магістратури. Констатовано, що у сучасному інформаційному суспільстві спостерігається залежність розвитку економічної, політичної та соціальної сфер від інформаційної та кібернетичної спроможності країни. Основну увагу зосереджено на аналізі нормативно-законодавчої бази у галузі кібербезпеки різних країн. Наголошено, що необхідності удосконалення нормативно-законодавчого забезпечення щодо регулювання процесів створення єдиного кіберпростору та освітнього простору між країнами ЄС, що сприятиме об'єднанню зусиль з кібернетичної безпеки країн-членів.*

*Розглянуто найбільш важливі закони та підзаконні акти, що розробляються міжнародними організаціями для удосконалення професійної підготовки магістрів з кібербезпеки. Визначено напрями удосконалення, зокрема: оновлення змісту освітніх та освітньо-наукових програм; розроблення рамкової моделі компетенцій для фахівців у галузі кібербезпеки; посилення інтеграції ІТ-освіти й науки; академічне визнання магістерських освітніх програм у ЄС. Виокремлено основні вимоги ЄС до професійної діяльності та професійної компетентності магістрів з кібербезпеки. З'ясовано, що перспективними цілями інтеграції країн ЄС у галузі підготовки магістрів з кібербезпеки є досягнення найвищого рівня професійної та академічної свободи, реформування ІТ-освіти.*

***Ключові слова:*** *професійна підготовка, магістратура, ІТ-фахівці, кібернетичний простір, кібербезпека, нормативно-законодавче забезпечення.*

У контексті інтеграції України у європейський освітній простір потребує реформування та модернізації система ІТ-освіти на рівні магістратури. Проблема підготовки конкурентоздатних ІТ-фахівців, зокрема магістрів з кібербезпеки, є важливим завданням для міжнародної академічної спільноти. Необхідність вирішення цієї проблеми особливо простежується на європейському рівні, що закріплено у низці нормативно-законодавчих ініціатив та активній діяльності відомих міжнародних організацій. На периферії наукових розвідок залишаються процеси стандартизації вищої ІТ-освіти. Об'єктивний аналіз педагогічних здобутків високорозвинених країн світу щодо особливостей професійної підготовки фахівців з кібербезпеки та їх творча

адаптація у вітчизняній практиці вищої школи сприятиме розширенню меж наукового пізнання щодо магістерської освіти, введенню нових педагогічних реалій та концептуальних підходів, модифікації системи вищої ІТ-освіти України.

Концептуальні засади розвитку ІТ-освіти та професійної підготовки фахівців в галузі кібербезпеки викладено в законодавчих і нормативно-правових актах нашої держави (Закон України "Про вищу освіту" (2014), "Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" (2007), Стратегія сталого розвитку "Україна – 2020 року" (2013), "Про Стратегію кібербезпеки України" (2017), "Про Національну програму інформатизації" (2012)).

Питання інформатизації суспільства та підготовки фахівців ІТ-галузі висвітлено у працях українських та зарубіжних науковців В. Бикова, К. Брюса (C. Bruce), Р. Гуревича, М. Кадемії, Е. Коена (E. Cohen), Т. Макгілла (T. McGill), Н. Нурієва, В. Сухомліна та ін. Специфіку розвитку вищої технічної освіти в зарубіжних країнах проаналізовано у наукових розвідках Л. Акімової, Н. Бідюк, Б. Бистрової, В. Третька, Р. Шарана, І. Пододіменко та ін.

Виділення невирішених раніше частин загальної проблеми. Транснаціональний характер кіберпростору вимагає вирішення проблем шляхом регіонального та міжнародного співробітництва. Водночас подолання загроз, розроблення відповідних рішень з метою зміцнення безпеки кіберпростору на міжнародному рівні зумовлює потребу у кооперації дій різних галузей: політичної, економічної, технологічної, освітньої, правової, управлінської, військової. Незважаючи на те, що національна політика будь-якої країни передбачає збереження і захист кордонів й національного суверенітету, інфраструктура, обладнання, та логістика кіберпростору функціонують поза межами цих кордонів, що надає йому міжнародного статусу.

Досвід європейських країн та світової спільноти показує, що вивчення, узагальнення і поширення інноваційних підходів у сфері професійної підготовки фахівців з кібербезпеки особливо ефективно здійснюється в межах міжнародних проектів. Це зумовлено необхідністю об'єднання перед проблемами кризових явищ і гуманітарних катастроф та створення спільних регуляційних та управлінських інституцій, вироблення єдиних стандартів, норм і правил здобуття освіти, безпекової політики тощо.

**Мета статті** полягає з'ясуванні нормативно-законодавчого регулювання професійної підготовки магістрів з кібербезпеки в умовах євроінтеграційних процесів та формування кібернетичного простору.

Глобальна інформатизація суспільства активізує нові геополітичні процеси, як-то: глобалізація економіки, що простежується у створенні транснаціональних корпорацій, міжнародному розподілі праці та ринків збуту продукції; глобалізація науки, що активізує створення розподілених міжнародних творчих колективів учених, які працюють над спільними науковими проектами, а також процес інтенсифікації міжнародного обміну науковою інформацією, проведення міжнародних телеконференцій;

глобалізація освіти, що активізує процес розвитку систем дистанційного навчання; глобалізація культури, яка проявляється у створенні електронних бібліотек, картинних галерей та інших творів мистецтва і літератури [9, с. 79-80; 10]

У сучасному інформаційному суспільстві спостерігається залежність розвитку економічної, політичної та соціальної сфер від інформаційної та кібернетичної спроможності країни. За підрахунками фахівців можливі збитки від кібератак на онлайнові-банківські та фінансові послуги лише однієї Європейської країни становлять понад 10 мільйонів євро на день [12]. Тому багато країн розробили та затвердили національну кібербезпекову стратегію, що була підкріплена відповідною законодавчою базою, та запровадили національні механізми реагування на кіберінциденти. Деякі країни проголосили кіберпростір п'ятим військовим об'єктом, а також створили захисні та наступальні кіберкоманди в своїх арміях задля мінімізації ризиків для промисловості та громадян.

Однак здійснений аналіз відповідних матеріалів свідчить про існування різних поглядів та підходів до вирішення проблеми кібернетичних загроз в різних країнах та залежності безпеки держави від якості вищої освіти. Відмінність спостерігається у визначенні відповідальних органів: якщо в одних країнах були створені національні організації, відповідальні за управління кібербезпекою, то в інших відповідальність за реалізацію національної політики покладена на координаційні органи, а управління та імплементація політики була залишена урядовим департаментам [1, с. 55-56].

Міжнаціональний характер кібернетичного простору потребує вироблення та координації політики передусім на міжнародному рівні. Вивчення оригінальних матеріалів дало змогу констатувати, що основними завданнями міжнародної політики в галузі розвитку кібербезпеки є: створення сприятливих умов для інтенсивного зростання інформаційного сектора національної економіки; підтримка інноваційних проектів створення та розвитку систем інформатизації в пріоритетних сферах інформатизації; забезпечення інформаційної безпеки та захисту інформації; забезпечення рівноправної участі в міжнародній відповідальності за глобальну або регіональну кібербезпеку; розвиток правової бази щодо створення міжнародного кодексу кібербезпеки; врегулювання різних аспектів функціонування кібернетичного простору.

Аналіз законодавчої бази у галузі кібербезпеки різних країн дав змогу з'ясувати, що вона є доволі складною і змінюється дуже швидко, причому різниця спостерігається у тому, як країни трактують кібербезпеку в національних законах. Багато країн та національних організацій дотримуються як національних, так і міжнародних законів з кібербезпеки і відповідно до них доповідають про певні типи фінансових або інших типів кіберзлочинів. Існують міжнародні норми правоохоронної діяльності (співпраця, запроваджена Інтерполом). Багатьма країнами були прийняті вимоги щодо інформування про скоєння кіберзлочинів. До найбільш впливових міжнародних організацій, що реалізують політику із координації і регулювання діяльності країн у галузі

безпечного використання кіберпростору, належать: ЮНЕСКО, НАТО, Кіберкоманда американського уряду (U.S. Government Cyber Command, Європол (Europol), Спільний центр досконалого кіберзахисту (Cooperative Cyber Defence Center of Excellence, CCD COE), Європейське агентство мереж та інформаційної безпеки (European Agency for Network and Information Security, ENISA), Міжнародна організація стандартизації (The International Organization for Standardization, ISO), Організація для безпеки та кооперації в Європі (Organisation for Security and Co-operation in Europe, OSCE), Міжнародний форум реагування на інциденти та командної безпеки (Global Forum for Incident Response and Security Teams), Міжнародне багатостороннє партнерство проти кіберзагроз (the International Multilateral Partnership Against Cyber Threats, IMPACT), Асоціація комунікації та електроніки озброєних сил (the Armed Forces Communications and Electronics Association, AFCEA), Інтернет корпорація присвоєння імен та номерів (the Internet Corporation for Assigned Names and Numbers, ICANN), Інтернет-форум управління (the Internet Governance Forum, IGF), Асоціація забезпечення безпеки інформаційних систем (ISSA).

Значну підтримку у розв'язанні проблем та сприянні розвитку ІТ-освіти надають такі міжнародні організації, як Асоціація обчислювальної техніки (ACM), Міжнародна асоціація комп'ютерних наук і інформаційних технологій (IACSIT), Асоціація професіоналів у галузі інформаційних технологій (AITP), Міжнародна асоціація фахівців з комп'ютерних досліджень (IACIS) та ін.

Перспективними цілями інтеграції країн Європи у галузі підготовки магістрів з кібербезпеки є такі: досягнення найвищого рівня професійної та академічної свободи, незважаючи на відмінності у системах загальної та вищої освіти; більша поступливість при взаємному визнанні термінів навчання і документів про закінчення навчальних закладів; сприяння вивченню іноземних мов, підвищення ролі інформаційних технологій у навчальному процесі; перехід до неперервної освіти; зближення загальної та спеціальної освіти; розширення доступу до вищих навчальних закладів; здійснення реформ ІТ-освіти.

Розглянемо найбільш важливі закони та підзаконні акти, що розробляються міжнародними організаціями для удосконалення професійної підготовки магістрів з кібербезпеки.

Організація Північноатлантичного договору (НАТО) є осередком колективної оборони, забезпечення кібербезпеки, розроблення механізмів запобіганню кіберзагроз, проведення міжнародних досліджень в галузі освіти з кібербезпеки тощо. У 2016 р. НАТО розробила важливий документ "Кібербезпека: навчальний план загального користування" (Cybersecurity: a generic reference curriculum) для забезпечення країн партнерів НАТО планом запровадження курсів та освітніх програм поглибленого вивчення проблем кібербезпеки. Цей документ є "дорожньої мапою" у процесі надання необхідних знань та навичок майбутнім фахівцям з кібербезпеки і дозволяє розвивати кібербезпекову політику на національному та міжнародному рівнях [11, с. 3]. Становить науковий і практичний інтерес визначені в документі

ключові компетентності фахівців з кібербезпеки та вимоги до професійної кваліфікації (навички управління кібероперaціями, знання кіберправа тощо), а також рекомендації щодо використання ефективних методів та форм навчання (проблемно-орієнтовані, практико-орієнтовані методи, залучення викладачів-практиків, відомих особистостей для обміну досвідом, лідерів приватних компаній тощо).Удосконалення нормативно-законодавчого забезпечення щодо регулювання процесів створення єдиного кіберпростору та освітнього простору між країнами ЄС сприятиме об'єднанню зусиль з кібернетичної безпеки країн-членів. Шляхом прийняття конвенцій, декларацій країни ЄС застосовують єдиний підхід у забезпеченні безпеки у кібернетичному просторі, визнаючи, таким чином, необхідність співпраці у цій галузі.

Найважливішим документом у галузі кібербезпеки є Конвенція Ради Європи про кіберзлочинність (Convention on Cybercrime) в рамках якої передбачено спільні заходи та процедурні інструменти (прийняття відповідного законодавства) країн щодо боротьби з кіберзлочинністю, ксенофобією та расизмом. Таким чином, Будапештська конвенція запроваджує міжнародні правові стандарти шляхом криміналізації кіберзлочинів, ініціює заходи для управління програмами боротьби з кіберзлочинністю, запроваджує співробітництво у виявленні, екстрадиції, взаємодопомоги, взаємообміну інформацією тощо [2, с. 10-17].

Інноваційним документом є Директива 2013/40/ ЄС Європейського Парламенту та Ради "Про напад на інформаційні системи" (Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems), якою запроваджено нові правила та покарання за кіберзлочинність. Основні види кримінальних злочинів, що визначені в цій Директиві, є напади на інформаційні системи, починаючи від атак про відмову в обслуговуванні, призначеної для знищення сервера, до перехоплення даних та атак ботнету. Таким чином, ця директива зосереджується на уніфікації кіберзлочинів для їх криміналізації у всіх державах-членах ЄС та співпраці правоохоронних органів [7].

З метою активізації реакції на терористичні акти у кіберпросторі ЄС у 2015 р. Радою ЄС була затверджена Європейська програма безпеки (The European Agenda on Security), в якій означені загальні стратегічні рамки ініціатив ЄС щодо забезпечення кібербезпеки та запобігання кіберзлочинності. Програма передбачає підвищення ефективності правоохоронних органів, зокрема шляхом створення Європейського центру боротьби з кіберзлочинністю (Європол), та вирішення проблем, пов'язаних із кримінальними розслідуваннями щодо кіберзлочинів, зокрема стосовно вільного доступу до доказів таких злочинів [5]. Основні заходи охоплюють такі напрями: посилення діалогу з ІТ-індустрією та зміцнення інструментів боротьби з кіберзлочинністю, підвищення якості ІТ-освіти, задоволення потреб галузі у кваліфікованих фахівцях, зміцнення потенціалу Європолу, підтримку дій міжнародних правоохоронних органів для боротьби з іноземними терористичними злочинцями тощо.

Рамкова політика ЄС щодо кіберзахисту (Cyber defence policy framework),

схвалена у 2014 р. Радою ЄС, є одним з головних документів, що стосуються питань протидії кіберзагрозам. Зокрема в документі визначено п'ять пріоритетних сфер для забезпечення кібернетичної безпеки та спільної політики захисту: підтримка розвитку можливостей кіберзахисту країн – членів союзу; сприяння співпраці між цивільною та військовою галуззями та поширення політики кіберзахисту в ЄС відповідними національними установами та установами ЄС; підвищення кваліфікації, забезпечення необхідної освіти та можливостей для навчання персоналу; посилення співпраці з відповідними міжнародними партнерами, зокрема НАТО [4].

Низка документів ЄС розроблена для об'єднання зусиль у безпечному користуванні кіберпростором. Заслуговує на увагу "Стратегія кібербезпеки ЄС: відкритий, безпечний кіберпростір" (Cybersecurity Strategy Of The European Union: An Open, Safe And Secure Cyberspace, 2013), в якій обґрунтовано стратегічні цілі та шляхи їх досягнення країнами ЄС у забезпеченні кіберстійкості; зниженні кіберзлочинності; розвитку відповідної національної політики та можливостей кіберзахисту, пов'язаних із спільною політикою безпеки та оборони; розвитку промислових та технологічних ресурсів для кібербезпеки; встановлення узгодженої міжнародної освітньої політики у сфері кібербезпеки для ЄС та сприяння розвитку основних цінностей [6].

Документ "Цифрова програма дій для Європи" (The Digital Agenda for Europe), що був прийнятий у травні 2010 р., є одним із найважливіших стратегічних документів на рівні ЄС, у якому підкреслюється загальне розуміння того, що довіра та безпека є фундаментальними передумовами поширення ІКТ та досягнення цілей "сталого зростання" відповідно до стратегії "Європа 2020". У розділі "Довіра та безпека" Програми відзначена необхідність об'єднання зусиль усіх зацікавлених сторін, спрямованих на безпеку та стійкість інфраструктури ІКТ, насамперед зосереджуючи увагу на запобіганні кіберзлочинам, готовності до захисту та обізнаності населення у цьому аспекті, достатньому кадровому забезпеченні галузі [3].

Важливо зазначити, що увага міжнародних організацій часто прикута до проблеми кадрового забезпечення ІТ-галузі та захисту кіберпростору. "Директива про мережеву та інформаційну безпеку" (The directive on network and information security), яка набрала чинності в серпні 2016 р. вимагає, щоб кожна держава – член ЄС – створила команду висококваліфікованих фахівців з питань своєчасного реагування на інциденти в галузі комп'ютерного захисту у межах спеціальної національної організації та запровадила співробітництво груп стратегічного співробітництва. Директива також гарантує поширення інформації між приватним та державним секторами та визначає декілька категорій операторів основних послуг, від яких вимагається прийняття відповідних заходів безпеки та повідомлення відповідних національних органів про серйозні інциденти, що мають місце у кіберпросторі [8].

З урахуванням аналізу вищезазначених міжнародних документів, визначено напрями удосконалення професійної підготовки магістрів з кібербезпеки: оновлення змісту освітніх та освітньо-наукових програм; окреслення загальних вимог до знань, умінь, поведінки та вимог до їхньої

професійної діяльності (загальносуспільні, морально-етичні, індивідуально-психологічні, практико-соціальні, фахові) і професійної компетентності (знання, професійні здібності, уміння, професійні й особистісні якості); узгодження змісту із потребами кіберполітики ЄС, а також із потребами особистості, науки і практики; створення професійно орієнтованого середовища для навчання; забезпечення високої якості практичної підготовки; орієнтація навчання на випереджувальний прогноз галузі; реалізація можливостей для професійного розвитку; створення мобільних груп до виконання завдань швидкого реагування та управління в кризових ситуаціях; організація регулярних експертних тренінгів з питань кризового менеджменту у кіберпросторі та надання практичних рекомендацій, проведення досліджень та організації міжнародних конференцій на тему співпраці в кіберпросторі; навчання протягом усього життя; впровадження наукових розробок в галузі кібербезпекових технологій; контроль якості кіберосвіти; академічне визнання освітніх програм у ЄС (професійна сертифікація) тощо.

**Висновки.** На підставі аналізу положень, викладених у міжнародних нормативно-правових документах, виокремлено основні вимоги ЄС до професійної діяльності та професійної компетентності магістрів з кібербезпеки, а саме: нормативно-правова кіберграмотність (високий рівень відповідальності за наслідки ухвалених рішень і дій; упровадження правових актів, що регулюють діяльність відповідних установ; розуміння процесів міжнародної кіберзлочинності; знання міжнародних практик та захист інтересів всіх суб'єктів, безпека навколишнього середовища); інформаційна та комп'ютерна грамотність (інформаційно-аналітичні здібності); організаційно-управлінські здібності (застосування інновацій в управлінні трудовими ресурсами, володіння інструментами управління ризиками, взаємодією з клієнтами); професійна та науково-дослідницька культура; комунікабельність (здатність підтримувати міжособистісні зв'язки, уміння вести переговори й ухвалювати правильні рішення, володіння іноземними мовами); психологічна готовність і лідерські якості (ініціативність, дух підприємництва, здатність до антиципації й врегулювання конфліктів, навички роботи в команді, дотримання норм професійної етики); здатність до навчання та професійного розвитку, саморефлексії.

Подальшими напрямами дослідження вважаємо розроблення рекомендацій щодо удосконалення стратегії кібербезпеки та системи ІТ-освіти в Україні з урахуванням досвіду країн ЄС.

***Використана література:***


1. Бистрова, Б. В. Професійна підготовка бакалаврів з кібербезпеки у вищих навчальних закладах США: дис. … канд. пед. наук : 13.00.04 - теорія і методика професійної освіти / Ін-т пед. освіти і освіти дорослих НАПН України. Київ, 2018. 259 с.
2. Council of Europe. (2001). Convention on Cybercrime, No. 185. Budapest, European Treaty Series, 22 p.
3. Council of Europe. (2010). A Digital Agenda For Europe, The European economic and social committee and the committee of the regions, 19 p.
4. Council of the European Union. (2014). Cyber defence policy framework, Brussels, 14 p.
5. Council of the European Union. (2015). The European agenda on security. Brussels, the European economic and social committee and the committee of the regions, 20 p.

6. European Commission. (2013). Cybersecurity Strategy Of The European Union: An Open, Safe And Secure Cyberspace. Brussels, The European economic and social committee and the committee of the regions, 20 p.
7. European Union. (2013). Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Official Journal of the European Union, L 218/8, 1-7.
8. European Union. (2016). Directives of the european parliament and of the council of 6 july 2016 concerning measures for a high common level of security of network and information systems across the Union the European Parliament the Council of the European Union, Official journal of the European Union, 194/1, 1-32
9. Masuda Y. (1990). Managing in the information Society : Releasing synergy Japanese style. Oxford. 293 p.
10. McCormick K. (2013). Engineers in Japan and Britain : Education, Training and Employment / K. McCormick. – Routledge. – 328 p.
11. NATO. (2016). Cybersecurity: a generic reference curriculum, Kingston, ON Canada: NATO graphics & printing, 72 p.
12. Radunović, V. (2013). DDoS - Available Weapon of Mass Disruption. Proceedings of the 21st Telecommunications Forum (TELFOR), P. 5-9.

***R e f e r e n c e s :***

[1] Bystrova, B. V. Profesiina pidhotovka bakalavriv z kiberbezpeky u vyshchykh navchalnykh zakladakh SShA [Professional training of bachelors in Cybersecurity in the US Higher Education Institutions]: dys. … kand. ped. nauk : 13.00.04 – teoriia i metodyka profesiinoi osvity / In-t ped. osvity i osvity doroslykh NAPN Ukrainy. Kyiv, 2018. 259 s. [in Ukrainian]
[2] Council of Europe. (2001). Convention on Cybercrime, No. 185. Budapest, European Treaty Series, 22 p.
[3] Council of Europe. (2010). A Digital Agenda For Europe, The European economic and social committee and the committee of the regions, 19 p.
[4] Council of the European Union. (2014). Cyber defence policy framework, Brussels, 14 p.
[5] Council of the European Union. (2015). The European agenda on security. Brussels, the European economic and social committee and the committee of the regions, 20 p.
[6] European Commission. (2013). Cybersecurity Strategy Of The European Union: An Open, Safe And Secure Cyberspace. Brussels, The European economic and social committee and the committee of the regions, 20 p.
[7] European Union. (2013). Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Official Journal of the European Union, L 218/8, 1-7.
[8] European Union. (2016). Directives of the european parliament and of the council of 6 july 2016 concerning measures for a high common level of security of network and information systems across the Union the European Parliament the Council of the European Union, Official journal of the European Union, 194/1, 1-32.
[9] Masuda Y. (1990). Managing in the information Society : Releasing synergy Japanese style. Oxford. 293 p.
[10] McCormick K. (2013). Engineers in Japan and Britain : Education, Training and Employment. Routledge. 328 p.
[11] NATO. (2016). Cybersecurity: a generic reference curriculum, Kingston, ON Canada: NATO graphics & printing, 72 p.
[12] Radunović, V. (2013). DDoS - Available Weapon of Mass Disruption. Proceedings of the 21st Telecommunications Forum (TELFOR), P. 5-9.

***БРАЙКО Б. В. Усовершенствование профессиональной подготовки магистров из кибербезопасности в условиях евроинтеграционных процессов.***

*Статья посвящена одной из актуальных проблем подготовки специалистов по кибербезопасности – реформированию и модернизации системы ИТ-образования на уровне магистратуры. Констатировано, что в современном информационном обществе наблюдается зависимость развития экономической, политической и социальной сфер от информационной и*

*кибернетической возможности страны. Основное внимание сосредоточенно на анализе нормативно-законодательной базы в отрасли кибербезопасности разных стран. Отмечено, что необходимости усовершенствования нормативно-законодательного обеспечения относительно регулирования процессов создания единственного киберпространства и образовательного пространства между странами ЕС, который будет способствовать объединению усилий по кибернетической безопасности стран-членов.*

*Рассмотрены наиболее важные законы и подзаконные акты, которые разрабатываются международными организациями для усовершенствования профессиональной подготовки магистров из кибербезопасности. Определенно направления усовершенствования, в частности: обновление содержания образовательных и образовательно-научных программ; разрабатывание рамочной модели компетенций для специалистов в отрасли кибербезопасности; усиление интеграции ИТ-образования и науки; академическое признание магистерских образовательных программ в ЕС. Выделены основные требования ЕС к профессиональной деятельности и профессиональной компетентности магистров из кибербезопасности. Выяснено, что перспективными целями интеграции стран ЕС в отрасли подготовки магистров из кибербезопасности являются достижения наивысшего уровня профессиональной и академической свободы, реформирования ИТ-образования.*

***Ключевые слова:*** *профессиональная подготовка, магистратура, ИТ-специалисты, кибернетическое пространство, кибербезопасность, нормативно-законодательное обеспечение.*

***Braiko B. V. Improving the Professional Training of Masters in Cyber Security in the Conditions of European Integration Processes.***

*The article deals with the problem of the professional training of Masters in Cyber Security, reforming and modernizing the IT education system at the level of master's level. It is stated that in the modern information society the dependence of the development of the economic, political and social spheres on the information and cybernetic capacity of the country is observed. The main focus is on the analysis of the regulatory framework in the field of cyber security in different countries. It was noted that there is a need to improve regulatory support for regulating the processes of creating a single cyberspace and educational space between EU countries, which will help to unite efforts on the cyber security.*

*The most important laws and regulations developed by international organizations to improve the professional training of Masters in Cyber Security are considered. Areas of improvement have been identified, in particular: updating the content of educational and educational-scientific programs; developing a competency framework for cyber security professionals; enhancing the integration of IT education and science; academic recognition of Master's degree programs in the EU. The basic requirements of the EU for the professional activity and professional competence of Masters in Cyber Security are highlighted. It has been found out that the achievement of a high level of professional and academic freedom and reform of IT education is a promising goal for the integration of EU countries in the preparation of Masters in Cyber Security.*

***Keywords:*** *training, Master's degree, IT-specialists, cyberspace, cyber security, regulatory and legislative support.*