УДК 378.016
DOI:

Юлія Сачук, *кандидат педагогічних наук, старший викладач кафедри комп'ютерних технологій та професійної освіти Луцького національного технічного університету*

НОРМАТИВНО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ФАХІВЦІВ ІЗ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Стаття присвячена розгляду проблеми якісної професійної підготовки фахівців із кібербезпеки та захисту інформації через правову призму. Процес професійної підготовки фахівців кібербезпеки та захисту інформації в Україні проходить період становлення та потребує досліджень й стандартизації. На основі аналізу трьох ключових нормативно-правових актів було виокремлено завдання щодо забезпечення кібербезпеки та захисту інформації у державі, що можуть бути вирішеними із залученням закладів вищої освіти, причому це сприятиме підвищенню ефективності професійної підготовки майбутніх фахівців із обраного профілю. Запропоновані конкретні рішення щодо розв'язання визначених питань.

Ключові слова: *фахівці із кібербезпеки та захисту інформації; професійна освіта; професійна підготовка; нормативно-правові засади.*

Табл. 2. Літ. 9.

Yuliya Sachuk, *Ph.D.(Pedagogy), Senior Lecturer of the Computer Technologies and Vocational Education Department Lutsk National Technical University*

THE NORMATIVE AND LEGAL BASIS OF PROFESSIONAL PREPARATION OF SPECIALISTS IN CYBER SECURITY AND PROTECTION OF INFORMATION

The article is devoted to the problem of qualitative professional training of specialists in cybersecurity and information protection through legal prism. One of the consequences of global informatization of state and military structures was the emergence of a fundamentally new environment of confrontation of competing states named cyberspace.

The purpose of the article is to identify and analyze the legal and regulatory framework for providing the high-quality professional training of specialists in cybersecurity and information security, formulating of proposals for improving the professional training of specialists of the selected profile.

The process of professional training of specialists of cyber security and information security in Ukraine is under development and requires research and standardization. In our opinion, the analysis of normative legal acts will determine the main ways of improving the training of professionals of the selected profile.

Based on the analysis of three key regulations, the author distinguished the task of ensuring cybersecurity and information security in the country that can be solved with the involvement of higher education institutions. This will increase the effectiveness of the training of future specialists of the selected profile. The specific solutions were proposed for solving the certain issues:

1) Creation of consulting points on cybersecurity and information protection on the basis of higher school. 2) Creation of training cybercenters. 3) Creation of expert groups of scientists. 4) An organization of courses on improving the digital literacy and cultural behavior in cyberspace for everyone. 5) It was proposed areas of activity for which it is expedient to develop the educational professional programs "Professional cybersecurity (in specialization)". 6) The involvement of the members of the National Academy of Sciences of Ukraine and foreign scientists in the field of cyber security and information protection training in the educational process. 7) An organization of the thematic scientific-practical and methodological conferences.

The prospects for further scientific research will address the organizational and methodological support of the proposed solutions.

Keywords: *the specialists in cybersecurity and information security; the vocational education; the professional training; the normative and legal principles.*

Постановка проблеми. Глобальна інформатизація у сьогоденні здійснює активну управлінську функцію існуванням та життєдіяльністю держав світового співтовариства, інформаційні технології застосовуються при вирішенні завдань забезпечення національної, військової та економічної безпеки. Разом із тим, одним із фундаментальних наслідків глобальної інформатизації державних та військових структур стало виникнення принципово нового середовища протиборства конкуруючих держав –

кіберпростору, який не є географічним у загальноприйнятому розумінні, але у повній мірі став міжнародним. На сьогодні питання щодо міжнародного паритету та взаємовідношень у кіберпросторі залишається відкритим.

У процесі формування глобального кіберпростору відбувається конвергенція військових та цивільних комп'ютерних технологій, у зарубіжжі інтенсивно розробляються нові засоби і методи активного впливу на інформаційну інфраструктуру, створюються різноманітні спеціалізовані кібернетичні центри та підрозділи управління, головною метою яких є захист державних та військових інформаційних інфраструктур, підготовка та проведення активних деструктивних дій в інформаційних системах противників та агресорів. Офіційні кібервійська уже функціонують у США, Китаї, Англії, Франції, Німеччині, Ізраїлі та ін.

У сучасних умовах проблема забезпечення кібербезпеки переходить із рівня захисту інформації на окремому об'єкті обчислювальної техніки на рівень створення єдиної системи кібербезпеки держави як складової системи інформаційної та національної безпеки, що відповідає не лише захисту інформації у вузькому розумінні, а й всього кіберпростору.

Процес професійної підготовки фахівців кібербезпеки та захисту інформації в Україні проходить період становлення та потребує досліджень й стандартизації. На наш погляд, аналіз нормативно-правових актів дозволить визначити основні шляхи удосконалення підготовки професіоналів обраного профілю.

Аналіз основних досліджень і публікацій. Проблемою підготовки фахівців із кіберзбезпеки переймались низка вітчизняних дослідників. В.Л. Бурячок та В.М. Богуш обґрунтовують необхідність запровадження профілю "Кібернетична безпека" через необхідність задоволення потреб силових структур, виробничої та банківської сфери України, а також проводять аналіз стандартів вищої освіти України за галуззю знань "Інформаційна безпека" [1]. У дослідженні І. Діордіца здійснено визначення напрямків підготовки та підвищення кваліфікації фахівців із кібербезпеки на основі системного аналізу освітніх систем. Серед векторів удосконалення фахової підготовки професіоналів досліджуваного профілю визначені здобуття другої вищої освіти, застосування нелінійної схеми підготовки фахівців за різними ступенями освіти, запровадження спеціалізацій із кібернетичної безпеки на інших спеціальностях (юридичних, економічних, управлінських тощо), перепідготовка в контексті післядипломної освіти фахівців із близькоспоріднених із кібернетичною безпекою спеціальностей; використання потенційних можливостей неформальної освіти для підвищення кваліфікації діючих фахівців через проведення тренінгів, круглих столів, міжнародних стажувань тощо [3]. Автор розкриває також тему ефективності та відповідності нормам освітніх стандартів професійної підготовки фахівців із кібербезпеки. Серед структуроутворювальних складових концепції організації професійної підготовки фахівців із кібербезпеки С. Мельником визначено мотиваційну, гносеологічну, праксеологічну, інформаційно-технологічну, моніторингову та оцінно-рефлексивну [4]. В.Б. Чередниченко та І.А. Кулик вважають засвоєння студентами наборів предметно-спеціальних компетентностей, визначених стандартом викладання комп'ютерних наук Computer Science Curricula, редакція CS2013 (ACM/IEEE-CS) основним напрямком підготовки фахівців з кібербезпеки для поліції України [9]. Особливості підготовки фахівців із захисту інформації у кіберпросторі США описали С.В. Мельник, С.О. Воскобойніков та виділили головну особливість – "гнучкість" навчального процесу, орієнтованого на досягнення успіху, складання особистого навчального плану та реалізації схеми індивідуального наставництва [2]. Здійснений аналіз не вичерпує результати усіх досліджень щодо професійної підготовки фахівців із кібербезпеки та захисту інформації.

Метою статті є виявлення та аналіз нормативно-правових засад забезпечення якісної професійної підготовки фахівців із кібербезпеки та захисту інформації, формулювання пропозицій щодо удосконалення професійної підготовки фахівців обраного профілю.

Виклад основного матеріалу дослідження. Кіберпростір України є складовою світового кіберпростору. Загрози кібербезпеки для українського суспільства аналогічні загрозам, що мають місце в інших країнах, багато з них є прямим наслідком неправомірних дій зарубіжних кіберзлочинців та спецслужб. Зважаючи на умови гібридної війни, що точиться в Україні, це робить державу першочерговим об'єктом для негативних кібервпливів. При цьому, попередні базові комп'ютерні технології щодо інформаційної безпеки недостатні та уже не забезпечують належного рівня захищеності та функційної стабільності. У вказаному ракурсі нами прийняте рішення щодо пошуку шляхів удосконалення професійної підготовки фахівців із кібербезпеки та захисту інформації через призму законодавства.

Для реалізації державної політики відносно

захисту у кіберпросторі державних інформаційних ресурсів та інформації прийнятий Закон України № 2163-VIII "Про основні засади забезпечення кібербезпеки України" (від 05.10.2017) [5]. Даний нормативно-правовий акт став основою розвитку державної системи захисту від мережевих загроз. Ним визначені правові та організаційні принципи забезпечення захисту національних інтересів України у кіберпросторі, основні цілі, спрямування та принципи державної політики у сфері кібербезпеки, а також повноваження й обов'язки державних органів у цій сфері, основні принципи координації їх діяльності відносно забезпечення кібербезпеки. Важливим є визначення даним законом суб'єктів національної системи кібербезпеки, тобто державних органів та інших організацій, які забезпечуватимуть кібернетичну безпеку та захищатимуть інформацію. Таким чином, перед вищою школою постає завдання якісно підготувати фахівців, які б наповнили виявлені інстанції. Отже, суб'єктами національної системи кібербезпеки є наступні: Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, СБУ, Міністерство оборони та Генштаб ЗСУ, розвідувальні органи та НБУ. Законом також визначені повноваження та функції суб'єктів кібербезпеки у рамках своєї компетенції:

- проведення заходів щодо запобігання кіберпростору у військових, розвідувально-підривних, терористичних та інших протиправних й злочинних цілях;
- вияв та реагування на кіберінциденти й кібератаки, ліквідацію їх наслідків;
- інформаційний обмін відносно реалізованих та потенційних кіберзагроз;
- розробка та реалізація попереджувальних, організаційних, освітніх та інших заходів у сфері кібербезпеки, кібероборони та кіберзахисту;
- забезпечення проведення аудиту інформаційної безпеки, у тому числі, на підпорядкованих об'єктах;
- інші заходи щодо забезпечення розвитку та безпеки кіберпростору.

Таким чином, базуючись на визначених повноваженнях, можна працювати над удосконаленням освітніх програм та стандартів щодо підготовки фахівців із досліджуваного профілю, формувати нову парадигму професійної підготовки, здійснювати підбір найбільш доцільних технологій та методів навчання фахівців із кібербезпеки та захисту інформації, а також формувати метасередовище їх освітньої діяльності.

Структури-суб'єкти національної системи кібербезпеки окреслюють різні сфери професійної діяльності: військову, банківську, інформаційну, правову. Залежно від сфери застосування, завдання та цілі фахівців з кібербезпеки та захисту інформації різняться та деталізуються. У даному контексті актуалізується доцільність виокремлення різних спеціалізацій профілю "Кібербезпека". Істинність даного припущення обумовлюється й різноманіттям об'єктів, які доведеться захищати.

Кіберзахисту підлягають комунікаційні системи усіх форм власності, у яких обробляються національні інформаційні ресурси і які використовуються в інтересах органів державної власності та місцевого самоуправління, правоохоронних органів та військових формувань, у сферах електронного управління, електронних державних послуг, електронної комерції, електронного документообігу, а також об'єкти критичної інформаційної інфраструктури (КІІ). До об'єктів КІІ відносять підприємства, установи та організації у галузі енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах; у сферах водо-, газо- та електропостачання, виробництва продовольства, сільського господарства, охорони здоров'я. Також до об'єктів КІІ належать комунальні, аварійні та рятувальні служби, стратегічні підприємства, потенційно небезпечні для виробництва.

Закон [5] передбачає й державно-приватну взаємодію. Передбачено підвищення цифрової грамотності громадян та культури безпеки поведінки у кіберпросторі. Запланований обмін інформацією про кіберзагрози та координації команд реагування на комп'ютерні надзвичайні ситуації. Для громадян, представників промисловості та бізнесу будуть створені консультаційні пункти.

Вважаємо, що створення консультаційних пунктів доцільно організувати на базі ЗВО. У рамках навчання в магістратурі, студенти спеціальності "Кібербезпека" зможуть удосконалити свій фаховий рівень завдяки вирішенню реальних практичних проблем, що виникають у осіб, що звертаються за допомогою.

Крім того, заплановане створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності щодо питань кібербезпеки.

Отже, перед вищою школою відкривається ціле поле нез'ясованих питань щодо підготовки фахівців кібербезпеки та захисту інформації для кожної із зазначених досить вузьких галузей діяльності.

Таблиця 1.

Способи вирішення завдань щодо забезпечення кібербезпеки України

Завдання	Спосіб вирішення
"…формування конкурентного середовища у сфері електронних комунікацій, наданні послуг із захисту інформації та кіберзахисту" [8, п.4.1]	Надання послуг із захисту інформації та кіберзахисту магістрантами зі спеціальності "Кібербезпека" у рамках проходження практики (робота у консультаційних пунктах на базі ЗВО)
"…залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки" [8, п.4.1]	Створення експертних груп науковців, до яких залучатимуться вітчизняні та зарубіжні учені та педагоги.
"…підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і здібностей, необхідних для підтримки цілей кібербезпеки, впровадженні державних і громадських проектів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту" [8, п.4.1]	Організація курсів підвищення кіберграмотності громадян, які проводитимуть магістранти спеціальності "Кібербезпека" у рамках практики. Підвищення кваліфікації існуючих фахівців з інформаційно-комунікаційних технологій, перекваліфікація кадрів, зацікавлених у формуванні безпечного кіберпростору держави. Здобуття кібернетичної освіти працівниками поліції.

Ґрунтуючись Законом України [5], вбачаємо першочерговим завданням організацію системи підготовки фахівців із кібербезпеки у військовій, банківській, енергетичній, правовій, економічній, сільськогосподарській, освітній сфері, бізнесі, логістиці, промисловості, енергетиці, журналістиці, аудиті.

Таким чином, актуалізується проблема розробки освітньо-професійних програм "Професійна кібербезпека (за спеціалізаціями)" для підготовки вузькопрофільних фахівців із кібербезпеки та захисту інформації. Із цього постає також питання щодо підготовки науково-педагогічних кадрів, які навчатимуть студентів із цих профілів. Необхідність розрізнення спеціалізацій із спеціальності "Кібербезпека" обумовлена тим, що кожна вузька галузь має специфічні характеристики, різноспрямовані та різнофункціональні програмні системи. Тому саме обізнаність у тонкощах кожної сфери діяльності дозволить виявити слабкі місця та вразливості у цих програмних системах, запобігти кібератакам чи оперативно усунути їх наслідки у разі виникнення.

Указом Президента України від 15.03.2016 "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [8] було введено у дію рішення Ради національної безпеки і оборони України та затверджено Стратегію кібербезпеки України. У даному документі акцентують на пріоритетах та напрямах забезпечення кібербезпеки України. Ті з них, які можуть бути певною мірою вирішені закладами вищої освіти, виокремлено у Таблиці 1.

Важливим нормативно-правовим актом, що стосується нашого дослідження, є Розпорядження Кабінету Міністрів України від 11 липня 2018 р. "Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України" [6]. У рамках документу можна виділити ряд заходів, які можна організовувати на базі ЗВО та які одночасно сприятимуть реалізації Стратегії кібербезпеки України й підвищуватимуть ефективність підготовки майбутніх фахівців обраного профілю (Таблиця 2).

Висновки і перспективи подальших розвідок. У рамках статті було проаналізовано три ключові нормативно-правові акти стосовно врегулювання питання кібербезпеки та захисту інформації в Україні: Закон України "Про основні засади забезпечення кібербезпеки України", Указ Президента України "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" та Розпорядження Кабінету Міністрів України "Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України". У результаті дослідження виявлено аспекти, що можуть бути вирішеними за допомогою потужностей закладів вищої освіти. Запропоновано різномасштабні рішення щодо їх реалізації:

- створення консультаційних пунктів з питань кібербезпеки та захисту інформації на базі ЗВО;
- створення тренінгових кіберцентрів;
- створення експертних груп науковців;
- організація курсів щодо підвищення цифрової грамотності та культури поводження у кіберпросторі для усіх бажаючих;

Таблиця 2.

Способи проведення заходів для реалізації Стратегії кібербезпеки України

Назва заходу	Спосіб реалізації у ЗВО
Опрацювання питання щодо утворення тренінгового кіберцентру в інтересах суб'єктів забезпечення кібербезпеки [6]	Створення локальних тренінгових кіберцентрів у ЗВО, у яких здійснюється професійна підготовка фахівців із кібербезпеки та захисту інформації; проведення базових тренінгів типу "Вступ до кібербезпеки", "Кібербезпека: основні поняття", "Кіберпростір: можливості та вразливості та ін." та міждисциплінарних тренінгів, наприклад, "Кібербезпека у бізнесі", "Кібербезпека й аудит", "Професійна кібербезпека", "Безпечний кібербанкінг" та ін. До проведення тренінгів варто залучати викладачів, науковців ЗВО, фахівців міжнародного рівня. До коучингу варто залучати студентів спеціальності "Кібербезпека", які зможуть випробовувати себе як у ролі слухачів, так і в ролі коучів. Спілкування із провідними фахівцями галузі сприятиме розвитку соціально-професійної мобільності студентів [7]. Ефективним буде також організувати співпрацю із професіоналами з ISSP Тренінг-центру, переймати їх успішний досвід та залучати до проведення тренінгів.
Вдосконалення механізму взаємодії з Національною академією наук та її профільними установами з метою проведення наукових досліджень та спільних науково-практичних робіт у галузях кібербезпеки та кіберзахисту критичної інфраструктури [6]	Залучення у навчальний процес підготовки фахівців із кібербезпеки та захисту інформації членів НАН України у ролі керівників науково-дослідних проектів магістрантів із досліджуваної спеціальності та консультантів для здобувачів наукових ступенів; лекторів для проведення наукових семінарів із даної тематики.
Розроблення методики формування та визначення основних показників ефективності реалізації Стратегії кібербезпеки України з урахуванням досвіду європейських і світових практик [6]	Проведення теоретичних, методичних та експериментальних досліджень у рамках курсових, дипломних, магістерських робіт; публікації результатів досліджень у фахових виданнях; проходження міжнародних стажувань із кібербезпеки для підвищення кваліфікації науково-педагогічних кадрів, що готують фахівців із кібербезпеки та захисту інформації.
Організація та проведення конференцій, семінарів, форумів, засідань круглих столів, тренінгів, навчань з питань кібербезпеки та кіберзахисту на державному і міжнародному рівнях [6]	Організація тематичних науково-практичних та методичних конференцій, круглих столів, форумів на базі ЗВО із залученням зарубіжних науковців та фахівців із кібербезпеки та захисту інформації.
Розвиток системи підготовки кадрів у сфері кібербезпеки, зокрема, підготовка фахівців тактичного та оперативно-тактичного рівня за напрямом "кібербезпека"; підготовка, атестація, переатестація та підвищення кваліфікації фахівців у сфері кіберзахисту для потреб державних органів, військових формувань і правоохоронних органів [6].	Відкриття спеціальності "Кібербезпека" у військових ЗВО; відкриття військових кафедр у ЗВО, де здійснюється підготовка фахівців обраного профілю.

- запропоновано сфери діяльності, для яких доцільно розробити освітньо-професійні програми "Професійна кібербезпека (за спеціалізаціями)";

- залучення у навчальний процес підготовки фахівців з кібербезпеки та захисту інформації членів НАН України та зарубіжних науковців із галузі;

- організація тематичних науково-практичних та методичних конференцій.

Перспективи подальших наукових розвідок стосуватимуться організаційно-методичного супроводу запропонованих рішень. На нашу думку, їх реалізація та впровадження стане значним кроком вперед у забезпеченні національної кібербезпеки України.

ЛІТЕРАТУРА

1. Бурячок В. Л. Рекомендації щодо побудови та запровадження профілю навчання "кібернетична

безпека" в Україні / В. Л. Бурячок, В. М. Богуш / Безпека інформації. – 2014. – Т. 20. – С. 126–131.

2. Воскобойніков С. О. Особливості професійної підготовки майбутніх фахівців із захисту інформації у кіберпросторі в Сполучених Штатах Америки / С. О. Воскобойніков, С. В. Мельник. // Педагогічна теорія і практика. – 2017. – №1. – С. 328–345.

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

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

5. Про основні засади забезпечення кібербезпеки України [Електронний ресурс]: Закон України від 05.10.2017 № 2163-VIII – Режим доступу: http://zakon2.rada.gov.ua

6. Розпорядження Кабінету Міністрів України від 11 липня 2018 р. "Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України" [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/481-2018-%D1%80

7. Сачук Ю. Є. Формування соціально-професійної мобільності майбутніх викладачів інформатики в процесі магістерської підготовки: дис. канд. пед. наук: 13.00.04 / Юлія Євгеніївна Сачук. – Луцьк, 2017. – 267 с.

8. Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/96/2016

9. Чередниченко В. Б. Визначення напрямків підготовки фахівців з кібербезпеки для поліції / В. Б. Чередниченко, І. А. Кулик // Підготовка охоронців правопорядку (1917-2017рр.): зб наук ст. і тез наук. практ. конф. до 100 – річчя підготовки охоронців правопорядку в Харкові (м. Харків 25 листопада 2017 р.) / МВС України, Харків. нац. ун-т внутр. справ. – Харків, 2017. – С.306–307.

REFERENCES

1. Buryachok, V. L. & Bohush, V. M. (2014). Rekomendatsiyi shchodo pobudovy ta Zaprovadzhennya profilyu navchannya "kibernetychna bezpeka" v Ukrayini [Recommendations for the construction and introduction of a cybernetic security training profile in Ukraine]. *Information security,* Vol. 20, pp. 126–131.[in Ukrainian].

2. Voskoboynikov, S. O. & Melnyk, S. V. (2017). Osoblyvosti profesiynoyi pidhotovky maybutnikh fakhivtsiv iz zakhystu informatsiyi u kiberprostori v Spoluchenykh Shtatakh Ameryky [Peculiarities of the training of future specialists in the field of information security in cyberspace in the United States of America]. *Pedagogical theory and practice,* No.1, pp. 328–345. [in Ukrainian].

3. Diorditsa, I. (2017). Napryamy pidhotovky ta pidvyshchennya kvalifikatsiyi fakhivtsiv iz kiberbezpeky [Areas of training and advanced training of specialists in cybersecurity]. *Entrepreneurship, economy and law,* No.3, pp. 199–203. [in Ukrainian].

4. Melnyk, S. (2016). Kontseptualni osnovy orhanizatsiyi profesiynoyi pidhotovky maybutnikh fakhivtsiv iz kiberbezpeky [Conceptual Foundations for the Professional Training of Future Cybersecurity Professionals]. *Pedagogical sciences: theory, history, innovative technologies,* No.10, pp. 79–88. [in Ukrainian].

5. Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny [About the basic principles of providing cyber security of Ukraine]. [Electronic resource]. Law of Ukraine dated 05.10.2017 № 2163-VIII, Access mode: http://zakon2.rada.gov.ua [in Ukrainian].

6. Rozporyadzhennya Kabinetu Ministriv Ukrayiny vid 11 lypnya 2018 r. "Pro zatverdzhennya planu zakhodiv na 2018 rik z realizatsiyi Stratehiyi kiberbezpeky Ukrayiny" [The Order of the Cabinet of Ministers of Ukraine dated July 11, 2018 "On Approval of the Plan of Measures for 2018 on the Implementation of the Cybersecurity Strategy of Ukraine"]. [Electronic resource]. Access mode: http://zakon.rada.gov.ua/laws/show/481-2018-%D1%80 [in Ukrainian].

7. Sachuk, Yu. Ye. (2017). Formuvannya sotsialno-profesiynoyi mobilnosti maybutnikh vykladachiv informatyky v protsesi mahisterskoyi pidhotovky [Formation of social and professional mobility of future teachers of computer science in the process of master's training]. *Candidate's thesis.* Lutsk, 267 p. [in Ukrainian].

8. Ukaz Prezydenta Ukrayiny Pro rishennya Rady natsionalnoyi bezpeky i oborony Ukrayiny vid 27 sichnya 2016 roku "Pro Stratehiyu kiberbezpeky Ukrayiny" [Decree of the President of Ukraine On the decision of the Council of National Security and Defense of Ukraine dated January 27, 2016 "On the Strategy of Cybersecurity of Ukraine"]. [Electronic resource]. Access mode: http://zakon0.rada.gov.ua/laws/show/96/2016 [in Ukrainian].

9. Cherednychenko, V. B. & Kulyk, I. A. (2017). Vyznachennya napryamkiv pidhotovky fakhivtsiv z kiberbezpeky dlya politsiyi [Identification of training courses for cyber security specialists for the police]. *Pidhotovka okhorontsiv pravoporiadku (1917 – 2017 rr.): zb nauk st. i tez nauk. prakt. konf. do 100 – richchia pidhotovky okhorontsiv pravoporiadku v Kharkovi (m. Kharkiv 25 lystopada 2017 r.)* – Training of Law Enforcement Guards (1917-2017). Associate Degrees of Science and Sciences. Pract Conf. to the 100th anniversary of the training of law enforcement guards in Kharkiv (Kharkiv, November 25, 2017). Ministry of Internal Affairs of Ukraine, Kharkiv, pp.306–307. [in Ukrainian].

Стаття надійшла до редакції 05.11.2018