

УДК 342.9

Ігор Діордіца,*канд. юрид. наук, доцент,
голова Інституту адміністративного правосуддя
Глобальної організації союзницького лідерства*

НАПРЯМИ ПІДГОТОВКИ ТА ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ ФАХІВЦІВ ІЗ КІБЕРБЕЗПЕКИ

Статтю присвячено визначенню напрямів підготовки й підвищення кваліфікації фахівців із кібербезпеки на основі системного аналізу. Встановлюються нормативно-правові засади щодо галузей знань і спеціальностей, за якими здійснюється підготовка фахівців із кібербезпеки, узагальнюється досвід провідних держав світу в цьому напрямі, обґрунтовуються пропозиції щодо запровадження варіантів підготовки та спеціалізацій, пов'язаних із професійною діяльністю у сфері кібернетичної безпеки, у межах суміжних галузей знань і спеціальностей.

Ключові слова: кібернетична безпека, підготовка фахівців із кібербезпеки, підвищення кваліфікації фахівців із кібербезпеки.

Постановка проблеми. Підготовка висококваліфікованих кадрів залишається ключовим елементом повноцінної життєдіяльності держави. Цей процес характеризується поєднанням потреб суспільства з технологіями дидактичного проектування з подальшим закріпленням на рівні нормативно-правових актів. Оскільки підготовка та підвищення кваліфікації фахівців із кібербезпеки є відносно новим видом діяльності, виникає потреба в науковому обґрунтуванні цих напрямів із позицій системного підходу.

Аналіз останніх досліджень і публікацій. Прийняттю постанови Кабінету Міністрів України, якою затверджується перелік галузей знань і спеціальностей [1], відповідних наказів Міністерства освіти і науки України [2] передує кропітке наукове дослідження самого механізму визначення економічних потреб держави на ринку праці [3], проектування освітніх систем на педагогічних засадах, методології встановлення диференційованих ознак, на підставі яких виділяються напрями, спеціальності й спеціалізації підготовки фахівців [4; 5]. Окремі аспекти здобуття освіти майбутніми фахівцями з кібербезпеки, питання підвищення кваліфікації, перепідготовки, спеціалізації діючих професіоналів знайшли відображення в наукових працях таких учених, як В. Бурачок [6], Ю. Даник і Ю. Супрунов [7], С. Демедюк і В. Марков [8], С. Мельник [9], А. Міночкін [10], Р. Прокуровський [11] та інші.

Окремо варто виділити науковий доробок Глобальної організації союзницького лідерства, зокрема й наукової школи доктора юридичних наук В. Ліпкана (її представляють 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. Туник, К. Череповський, О. Шепета та інші вчені). У роботах цих авторів закладено фундамент для формування

сучасних напрямів підготовки фахівців із кібербезпеки [12–21].

Попри наявність публікацій щодо проблемних питань навчання фахівців із кібернетичної безпеки, на засадах системного аналізу визначення напрямів підготовки й підвищення кваліфікації цієї категорії професіоналів не проводилось. Також варто враховувати, що після прийняття 29 квітня 2015 р. постанови Кабінету Міністрів України № 266 (зі змінами від 27 вересня 2016 р. згідно з постановою № 674), якою затверджений перелік галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти [1], наукові дослідження в аспекті окресленої проблематики не здійснювались.

Метою статті є визначення напрямів підготовки та підвищення кваліфікації фахівців із кібербезпеки на основі системного аналізу освітніх систем.

Досягнення поставленої мети потребує вирішення таких завдань: 1) встановлення нормативно-правових засад щодо галузей знань і спеціальностей, за якими здійснюються підготовка й підвищення кваліфікації фахівців із кібербезпеки; 2) узагальнення досвіду провідних держав щодо напрямів підготовки професіоналів зазначеної категорії; 3) обґрунтування пропозицій щодо запровадження варіантів підготовки та спеціалізацій, пов'язаних із професійною діяльністю у сфері кібернетичної безпеки, у межах суміжних галузей знань і спеціальностей.

Виклад основного матеріалу дослідження. Феномен кібернетичної безпеки полягає в її бінарному характері. З одного боку, вона може розглядатись як елемент національної безпеки. З іншого боку, з огляду на те, що інформаційний простір є безмежним, для нього не існує кордонів, тому злочини в цій сфері здебільшого кваліфікуються як транснаціональні, а отже, кібернетичну безпеку варто розглядати як явище глобалізоване. Це означає, що питання підготовки та підвищення кваліфікації фахівців у

зазначеній галузі є принципово важливим не лише для України, а й для світової спільноти загалом.

Правова регламентація цих процесів здійснюється на основі Закону України «Про освіту» та Закону України «Про вищу освіту». Зокрема, відповідно до статті 13 Закону України «Про вищу освіту» на центральний орган виконавчої влади у сфері освіти й науки, інші органи, до сфери управління яких належать вищі навчальні заклади, покладаються також такі функції, як проведення аналітико-прогностичної діяльності у сфері вищої освіти, визначення тенденцій її розвитку, впливу демографічної, етнічної, соціально-економічної ситуації, інфраструктури виробничої й невиробничої сфери, формування стратегічних напрямів розвитку вищої освіти з урахуванням науково-технічного прогресу та інших факторів, узагальнення світового й вітчизняного досвіду розвитку вищої освіти [22]. Також цим законом передбачається, що Міністерство освіти і науки України (далі – МОН України) «формує перелік галузей знань і перелік спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, зокрема за поданням Національного агентства із забезпечення якості вищої освіти, та подає їх на затвердження Кабінету Міністрів України» [22].

З огляду на наведену норму основними суб'єктами формування переліків галузей знань і спеціальностей виступають МОН України та Національне агентство із забезпечення якості вищої освіти (далі – НАЗЯВО). Можливо, саме такий підхід дає змогу певною мірою оптимізувати занадто деталізовані й кількісно переобтяжені переліки, які нерідко призводили до широкої синонімії в спеціальностях і фактичного дублювання освітніх програм. Водночас, якщо йдеться про сферу забезпечення національної безпеки держави, у тому числі кібернетичної, коло суб'єктів, на яких покладаються обов'язки визначення напрямів підготовки фахівців, на нашу думку, має бути поширено. Принаймні важливою є позиція Ради національної безпеки і оборони України, тих державних інституцій, які здійснюють кадрове забезпечення відповідними фахівцями.

Загалом досить дискусійним є питання щодо ролі НАЗЯВО у формуванні переліку галузей знань і спеціальностей. Стаття 18 Закону України «Про вищу освіту» відображає широкі повноваження цього органу, який за семантикою назви покликаний сприяти максимальній ефективності освітнього процесу. Фактично ж в окремих позиціях НАЗЯВО перетворили на проміжний ланцюг між МОН України та вищими навчальними закладами, адже як інакше сприймати норму, що НАЗЯВО «формує за поданням вищих навчальних закладів (наукових установ) пропозиції, у тому числі з метою запровадження міждисциплінарної підготовки, щодо переліку спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти на відповідних рівнях вищої освіти, і подає його центральному органу виконавчої влади у сфері освіти й науки» [22].

Недооцінка ролі фахівців у формуванні переліків галузей знань і спеціальностей призвела до того, що в результаті низки трансформацій у Постанові Кабінету Міністрів України «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 29 квітня 2015 р. № 266 під шифром 125 залишилась лише спеціальність «Кібербезпека» в межах галузі знань «Інформаційні технології» [10]. На переконання укладачів документа, вказана спеціальність поглинула чинну в попередній постанові [23] галузь знань 1701 «Інформаційна безпека» з усіма її спеціальностями. На це вказують також таблиці переходів напрямів у галузі знань і спеціальностей, що містяться в додатках до наказу МОН України від 6 листопада 2015 р. № 1151 [2].

Подібна позиція є неприпустимою, оскільки поняття галузей «Інформаційна безпека» та «Кібербезпека» є спорідненими, проте не тотожними. Ми розподіляємо погляди С. Мельника з приводу того, що «предметна сфера інформаційної безпеки включає в себе широкий спектр питань щодо іміджу держави, забезпечення інформаційних прав і свобод громадян, забезпечення інформаційного суверенітету, захисту інформації, правоохоронної діяльності, відповідно, можна стверджувати й про адекватну «фахову широту» соціального замовлення на освіту в цій сфері» [9, с. 188].

Таким чином, виникає потреба в з'ясуванні кола осіб, яких можна віднести до категорії фахівців із кібербезпеки.

Наша наукова позиція базується на необхідності запровадження в інтерпретації цього поняття двох підходів – вузького та широкого.

Отже, у вузькому значенні термінологічного сполучення під фахівцями з кібернетичної безпеки можна розуміти осіб, які мають профільну освіту за спеціальністю «Кібербезпека» та працюють за фахом. Якщо суворо дотримуватись юридичних норм, то існують підстави відносити до вказаної категорії лише тих, хто опановував галузь «Інформаційні технології» за цією спеціальністю.

Безумовно, подібний підхід є занадто звуженим і суперечить елементарній логіці. Достатньо навіть простежити це на рівні того ж наказу МОН України [2], яким затверджується таблиця відповідності Переліку наукових спеціальностей (Перелік-2011) та Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти. Згідно з наведеними там відомостями особи, які здобули рівень магістра за спеціальністю 125 «Кібербезпека», можуть захищати дисертації на здобуття наукового ступеня кандидата наук (доктора філософії) і доктора наук за такими науковими спеціальностями: 21.05.01 «Інформаційна безпека держави», 21.07.01 «Забезпечення державної безпеки України», 21.07.02 «Розвідувальна діяльність органів державної безпеки». При цьому передбачається, що ця категорія фахівців можуть спеціалізуватись не тільки в технічній галузі, їм може присуджуватись науковий ступінь у галузі фізико-математичних, юридичних,

психологічних, військових, соціологічних, політичних наук. У подібній ситуації варто говорити про міждисциплінарність спеціальності «Кибербезпека», що підтверджує нашу думку про запровадження поняття «фахівець із кібербезпеки» в широкому розумінні.

На користь нашої наукової позиції слугує й факт добору кадрів для роботи в Департаменті кіберполіції Національної поліції України. Чітко відстежується потреба не лише у фахівцях технічного профілю, а й у правниках [24].

Досить показовим є також аналіз міжнародного досвіду. За спостереженнями М. Анур'євої, яка дослідила більше 400 програм підготовки бакалаврів і магістрів, доступних на сайтах вищих навчальних закладів США, Великої Британії, Німеччини, Франції, фахівець у сфері інформаційної безпеки, у тому числі кібернетичної, може стати бакалавром або магістром гуманітарних, природничих, технічних наук, магістром права або магістром філософії [25]. Цьому сприяє вивчення з-поміж інших таких курсів, як «Безпека інформаційних систем і фінансів», «Етичний хакінг у комп'ютерній

безпеці», «Законодавство у сфері комерційних інформаційних технологій», «Розслідування комп'ютерних інцидентів», «Біометрика та інформаційна безпека», «Криптографія» тощо.

Отже, ми пропонуємо, вживаючи термінологічне сполучення «фахівець із кібербезпеки» в широкому розумінні, іменувати так осіб, які за родом своєї професійної діяльності можуть використовувати спеціальні знання для попередження потенційних загроз, викриття/розкриття, нейтралізації або мінімізації наслідків протиправної поведінки правопорушників у комп'ютерному просторі. У такому контексті навіть викладача інформатики в школі або у вищому навчальному закладі можна вважати фахівцем із кібербезпеки, оскільки у своїй діяльності він покликаний не лише дати знання зі сфери інформаційних технологій, а й здійснюючи виховну роботу, виконувати превентивні функції. Подібний приклад означає, що кібернетична безпека може виступати не тільки як спеціальність, а й як спеціалізація в межах інших спеціальностей або як окрема компонента освітньої програми підготовки фахівця.

Таблиця 1

Проекція Конвенції Ради Європи про кіберзлочинність на зміст освіти за суміжними з кібербезпекою спеціальностями

Положення Конвенції Ради Європи про кіберзлочинність	Шифри, галузі знань, назви спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти
Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання в дані, у систему, зловживання пристроями)	08 «Право» – 081 «Право»; 12 «Інформаційні технології» – 124 «Системний аналіз»; 25 «Воєнні науки, національна безпека, безпека державного кордону»; 26 «Цивільна безпека» – 262 «Правоохоронна діяльність», 263 «Цивільна безпека»; 05 «Соціальні та поведінкові науки» – 051 «Економіка», 056 «Міжнародні економічні відносини»; 07 «Управління та адміністрування» – 071 «Облік і оподаткування», 072 «Фінанси, банківська справа та страхування», 073 «Менеджмент»
Правопорушення, пов'язані з комп'ютерами (підробка, шахрайство, пов'язані з комп'ютерами)	08 «Право» – 081 «Право»; 07 «Управління та адміністрування» – 071 «Облік і оподаткування», 072 «Фінанси, банківська справа та страхування», 073 «Менеджмент»
Правопорушення, пов'язані зі змістом (зокрема, дитяча порнографія, розповсюдження ідей расизму й ксенофобії)	08 «Право» – 081 «Право»; 03 «Гуманітарні науки» – 033 «Філософія»; 05 «Соціальні та поведінкові науки» – 052 «Політологія», 053 «Психологія», 054 «Соціологія», 055 «Міжнародні відносини, суспільні комунікації та регіональні студії»; 06 «Журналістика»; 01 «Освіта» – 011 «Науки про освіту»; 02 «Культура і мистецтво» – 021 «Аудіовізуальне мистецтво та виробництво», 028 «Менеджмент соціокультурної діяльності», 029 «Інформаційна, бібліотечна та архівна справа»; 23 «Соціальна робота»
Правопорушення, пов'язані з порушенням авторських та суміжних прав	08 «Право» – 081 «Право»; 02 «Культура і мистецтво» – 021 «Аудіовізуальне мистецтво та виробництво», 023 «Образотворче мистецтво, декоративне мистецтво, реставрація», 025 «Музичне мистецтво», 028 «Менеджмент соціокультурної діяльності»; 03 «Гуманітарні науки» – 034 «Культурологія», 035 «Філологія»
Міжнародне співробітництво з боротьби з кіберзлочинністю	08 «Право» – 082 «Міжнародне право»; 05 «Соціальні та поведінкові науки» – 055 «Міжнародні відносини, суспільні комунікації та регіональні студії»

На засадах концепції безперервної освіти можливі декілька варіантів роботи в цьому напрямі, а саме:

1) надання другої вищої освіти. Найбільш складний (з огляду на тривалість, вартість, вимоги до різносторонності задатків і здібностей здобувача вищої освіти), проте й найбільш дієвий шлях. Наприклад, випускник технічного вищого навчального закладу отримує другу вищу освіту за правничим фахом;

2) застосування нелінійної схеми підготовки фахівців за різними ступенями освіти, що стало можливим завдяки новим нормам, закріпленим у Законі України «Про вищу освіту». Наприклад, бакалавр технічного профілю вступає до магістратури за економічним фахом із метою подальшої роботи як фахівця з кібербезпеки в банківській сфері;

3) запровадження спеціалізацій із кібернетичної безпеки на інших спеціальностях (юридичних, економічних, управлінських тощо);

4) перепідготовка в контексті післядипломної освіти фахівців із близькоспоріднених із кібернетичною безпекою спеціальностей;

5) використання потенційних можливостей неформальної освіти для підвищення кваліфікації діючих фахівців через проведення тренінгів, круглих столів, міжнародних стажувань тощо.

Напрями підготовки й підвищення кваліфікації фахівців із кібербезпеки, на наше переконання, доцільно проектувати відповідно до Конвенції про кіберзлочинність, прийнятої Радою Європи 23 листопада 2001 р. (ратифікована Верховною Радою України 7 вересня 2005 р.) [16]. Кожен із виділених у ній аспектів може кореспондуватись зі змістом освіти за спеціальностями, за якими в Україні здійснюється підготовка здобувачів вищої освіти. У найбільш узагальненому вигляді таку інформацію доцільно представити у формі таблиці.

Наведений перелік не є вичерпним, хоча й достатньо повно демонструє, що об'єкт і предмет кібербезпеки настільки багатогранні, що забезпечити повноцінну діяльність лише фахівцями з однієї спеціальності практично неможливо. Особливої уваги потребує підготовка аналітиків у сфері кібернетичної безпеки, на яких мають покладатись обов'язки щодо виявлення криміногенних чинників, що сприяють розповсюдженню комп'ютерних злочинів, відстеження основних тенденцій і прогнозування потенційних загроз. Незважаючи на важливість цієї категорії фахівців, такої спеціальності в Україні сьогодні немає.

Висновки

Таким чином, у результаті проведеного аналізу вдалось встановити, що поняття «фахівець із кібербезпеки» не має обмежуватись лише тією групою осіб, які здобули вищу освіту за зазначеним фахом. Процес підготовки кадрів, підвищення їх кваліфікації в цьому напрямі з урахуванням всіх аспектів діяльності та сфер життя держави, у тому числі в галузі міжнародного співробітництва, має здійснюватись на

інтеграційних засадах кореляції всіх складників кібернетичної безпеки.

Список використаних джерел:

1. 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 № 674 від 27 вересня 2016 р.) [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/266-2015-%D0%BF>.

2. Про особливості запровадження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, затвердженого постановою Кабінету Міністрів України від 29 квітня 2015 р. № 266 : Наказ Міністерства освіти і науки України від 6 листопада 2015 р. № 1151 [Електронний ресурс]. – Режим доступу : <http://zakon0.rada.gov.ua/laws/show/z1460-15>.

3. Ринок праці України: перспективи євроінтеграції / [І. Гнибіденко та ін.] ; за ред. І. Гнибіденка. – К. : ДКС-центр, 2012. – 244 с.

4. Лігоцький А. Теоретичні основи проектування сучасних освітніх систем / А. Лігоцький. – К. : Техніка, 1997. – 209 с.

5. Шанскова Т. Професійна підготовка фахівців гуманітарного профілю в умовах другої вищої освіти: теорія і методика / Т. Шанскова ; за заг. ред. О. Дубасенюк. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 383 с.

6. Бурячок В. Проблемні питання та актуальні завдання підготовки фахівців з кібернетичної безпеки галузі знань «Інформаційні технології» / В. Бурячок, І. Пархомей, М. Степанов, В. Толубко // Сучасний захист інформації. – 2016. – № 2. – С. 4–9.

7. Даник Ю. Деякі підходи до формування системи підготовки кадрів для системи кібернетичної безпеки України / Ю. Даник, Ю. Супрунов // Збірник наукових праць Житомирського військового інституту Національного авіаційного університету. – 2011. – Вип. 5. – С. 5–22.

8. Демедюк С. Підготовка та підвищення кваліфікації працівників у сфері боротьби з кіберзлочинністю / С. Демедюк, В. Марков // Право.ua. – 2015. – № 1. – С. 48–52.

9. Мельник С. Понятійно-категоріальний апарат у системі професійної підготовки майбутніх фахівців з кібербезпеки / С. Мельник // Інформаційні технології і засоби навчання. – 2016. – Т. 55. – № 5. – С. 187–197.

10. Міночкін А. Інформаційна боротьба: сучасний стан та досвід підготовки фахівців / А. Міночкін // Оборонний вісник. – К. : Центр воєнної політики та політики безпеки, 2011. – № 2. – С. 12–14.

11. Проскурівський Р. Аналіз стану підготовки фахівців у галузі «Інформаційна безпека» / Р. Проскурівський // Прикладная радиоэлектроника. – 2013. – Т. 12. – № 2. – С. 303–307.

12. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції : [навч. посібник] / В. Ліпкан, Ю. Максименко, В. Желіховський. – К. : КНТ, 2006. – 280 с.

13. Систематизація інформаційного законодавства України : [монографія] / [В. Ліпкан, В. Залізняка] ; за заг. ред. В. Ліпкана. – К. : ФОП Ліпкан О.С., 2012. – 304 с.

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

15. Консолідація інформаційного законодавства України : [монографія] / [В. Ліпкан, М. Дімчогло] ; за заг. ред. В. Ліпкана. – К. : ФОП Ліпкан О.С., 2014. – 416 с.

16. Інкорпорація інформаційного законодавства України : [монографія] / [В. Ліпкан, К. Череповський] ; за заг. ред. В. Ліпкана. – К. : ФОП Ліпкан О.С., 2014. – 408 с.

17. Правові засади розвитку інформаційного суспільства в Україні : [монографія] / [В. Ліпкан, І. Сопілко, В. Кір'ян] ; за заг. ред. В. Ліпкана. – К. : ФОП Ліпкан О.С., 2015. – 664 с.

18. Правовий режим податкової інформації в Україні : [монографія] / [В. Ліпкан, О. Шепета, О. Мандзюк] ; за заг. ред. В. Ліпкана. – К. : ФОП Ліпкан О.С., 2015. – 440 с.

19. Стратегічні комунікації : [словник] / [Т. Попова, В. Ліпкан] ; за заг. ред. В. Ліпкана. – К. : ФОП Ліпкан О.С., 2016. – 416 с.

20. Мандзюк О. Правове регулювання аналітичної діяльності в Україні : [монографія] / О. Мандзюк, М. Сабіна. – К. : Дорадо-Друк, 2016. – 312 с.

21. Рудник Л. Право на доступ до інформації : дис. ... канд. юрид. наук : спец. 12.00.07 / Л. Рудник ;

Нац. ун-т біоресурсів і природокористування України. – К., 2015. – 247 с.

22. Про вищу освіту : Закон України від 1 липня 2014 р. (редакція від 30 листопада 2016 р.) [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/1556-18>.

23. Про затвердження напрямів і спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційними рівнями спеціаліста і магістра : Постанова Кабінету Міністрів України від 27 серпня 2010 р. № 787 (втратила чинність) [Електронний ресурс]. – Режим доступу : <http://zakon0.rada.gov.ua/laws/show/787-2010-p>.

24. Міністерство внутрішніх справ України оголошує конкурс на заміщення вакантних посад інспекторів та спеціалістів інформаційних технологій Департаменту кіберполіції [Електронний ресурс]. – Режим доступу : <https://www.npu.gov.ua/uk/publish/article/1668305>.

25. Анурьева М. О приоритетах образовательных программ в области информационной безопасности в разных странах / М. Анурьева // Психолого-педагогический журнал «Гуадеамус». – 2013. – № 1(21). – С. 102–109.

26. Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 р. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/994_575.

Статья посвящена определению направлений подготовки и повышения квалификации специалистов по кибербезопасности на основе системного анализа. Определяются нормативно-правовые основы отраслей знания и специальностей, по которым осуществляется подготовка специалистов по кибербезопасности, обобщается опыт ведущих государств мира в данном направлении, обосновываются предложения относительно вариантов подготовки и специализаций, связанных с профессиональной деятельностью в сфере кибернетической безопасности, в рамках смежных отраслей знаний и специальностей.

Ключевые слова: кибернетическая безопасность, подготовка специалистов по кибербезопасности, повышение квалификации специалистов по кибербезопасности.

The article is devoted to the identification of the directions of training and advanced training of specialists in cybersecurity on the basis of system analysis. The regulatory and legal foundations of the knowledge and specialties are determined, which train cybersecurity specialists, generalize the experience of the leading states of the world in this direction, justify proposals on training options and specializations related to professional activities in the field of cyber security in the framework of related fields of knowledge and specialties.

Key words: cyber security, cyber security training, advanced training of specialists in cybersecurity.