

**Звіт про громадське обговорення проєкту стандарту вищої освіти
третього (освітньо-наукового) рівня,
галузі знань 12 Інформаційні технології,
спеціальності 125 Кібербезпека та захист інформації**

1. Найменування органу виконавчої влади, який проводив обговорення:
Міністерство освіти і науки України.

2. Зміст питання або назва проєкту документу, що виносилися на обговорення:

Проєкт стандарту вищої освіти України третього (освітньо-наукового) рівня спеціальності 125 Кібербезпека та захист інформації галузі знань 12 Інформаційні технології (далі – проєкт Стандарту).

Розробка стандартів передбачена статтею 10 Закону України «Про вищу освіту».

Стандарт вищої освіти – це сукупність вимог до освітніх програм вищої освіти, які є спільними для всіх освітніх програм у межах певного рівня вищої освіти та спеціальності.

Стандарти вищої освіти розробляються для кожного рівня вищої освіти в межах кожної спеціальності відповідно до Національної рамки кваліфікацій і використовуються для визначення та оцінювання якості вищої освіти та результатів освітньої діяльності закладів вищої освіти (наукових установ), результатів навчання за відповідними спеціальностями.

Громадське обговорення проведено у формі електронних консультацій. Проєкт Стандарту було розміщено 18 серпня 2023 р. на офіційному вебсайті Міністерства освіти і науки України за посиланням:

<https://mon.gov.ua/ua/news/mon-proponuye-do-gromadskogo-obgovorennya-proyekt-standartu-vishoyi-osviti-zi-specialnosti-125-kiberbezpeka-ta-zahist-informaciyi-na-tretomu-osvitno-naukovomu-rivni-vishoyi-osviti>

Зауваження та пропозиції до проєкту Стандарту приймалися до 04 вересня 2023 р. на електронну адресу: mruga@mon.gov.ua.

3. Інформація про осіб, що взяли участь в обговоренні:

Впродовж встановленого для обговорення з громадськістю терміну надіслав зауваження та пропозиції один адресант: Певнев В.Я., Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут»

4. Інформація про пропозиції, що надійшли до Міністерства освіти і науки України за результатами обговорення:

Пропозиція Певнева В.Я., Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут».

У розділі II. Загальна характеристика → Опис предметної області → Інструменти та обладнання.

Програмно-апаратне та програмне забезпечення, інструментальні засоби, комп'ютерна техніка, спеціальні контрольно-вимірювальні прилади, програмно-технічні засоби автоматизації та системи автоматизації проектування, виробництва, експлуатації, контролю, моніторингу, мережні, мобільні, хмарні, технології, мережне

устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі кібербезпеки та захисту інформації.

Вилучити «а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі кібербезпеки та захисту інформації.» оскільки теорія та моделі не є «Інструментами та обладнанням».

У розділі V. Перелік компетентностей випускника

Інтегральну компетентність викласти в редакції:

«Здатність продукувати нові ідеї, розв'язувати комплексні проблеми професійної та/або дослідницько інноваційної діяльності у сфері кібербезпеки та захисту інформації, застосовувати методологію наукової та педагогічної діяльності, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення».

Спеціальні (фахові, предметні) компетентності:

СК-1. Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у сфері кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямках і можуть бути опубліковані у провідних наукових виданнях з кібербезпеки та захисту інформації **та суміжних галузей.**

Коментар: такі публікації не враховуються.

СК-3. Здатність усно і письмово презентувати та обговорювати результати наукових досліджень та/або інноваційних розробок українською та англійською мовами, глибоке розуміння англійських наукових текстів в галузі кібербезпеки та захисту інформації.

Викласти в редакції:

СК-3. Здатність усно і письмово презентувати та обговорювати результати наукових досліджень та/або інноваційних розробок державною та іноземною мовами, глибоке розуміння наукових текстів в галузі кібербезпеки та захисту інформації.

СК-4. Здатність здійснювати науково-педагогічну діяльність у вищій освіті.

Коментар: працевлаштування випускників значно ширше, тому пропонується викласти в редакції:

СК-4. Здатність здійснювати професійну, наукову, науково-педагогічну діяльність у підприємствах, наукових установах і закладах вищої освіти.

У розділі VI. Нормативний зміст підготовки здобувачів доктора філософії, сформульований у термінах результатів навчання

РН-6. Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми кібербезпеки та захисту інформації державною та іноземною мовами усно та письмово, оприлюднювати

результати досліджень у наукових публікаціях у провідних **міжнародних наукових виданнях**.

Додати «державних і міжнародних наукових виданнях»

РН-10. Організувати і здійснювати освітній процес у сфері інформаційних технологій, його наукове, навчально-методичне та нормативне забезпечення, розробляти і викладати спеціальні навчальні дисципліни у закладах вищої освіти.

Викласти в редакції:

РН-10. Організувати і здійснювати освітній процес у сфері кібербезпеки та захисту інформації, його наукове, навчально-методичне та нормативне забезпечення, розробляти і викладати спеціальні навчальні дисципліни у закладах вищої освіти.

У розділі VII. Форми атестації здобувачів вищої освіти → Вимоги до дисертації на здобуття ступеня доктора філософії

Перший абзац «Дисертація на здобуття ступеня доктора філософії є самостійним розгорнутим дослідженням, що пропонує розв'язання комплексної проблеми в сфері кібербезпеки та захисту інформації або на її межі з іншими спеціальностями, результати якого мають наукову новизну, теоретичне та практичне значення.»

Викласти в редакції:

Дисертація на здобуття ступеня доктора філософії є самостійним розгорнутим дослідженням, що пропонує розв'язання комплексної задачі в сфері кібербезпеки та захисту інформації, результати якого мають наукову новизну, теоретичне та практичне значення.

5. Інформація про рішення, прийняті за результатами обговорення:

Під час доопрацювання проєкту Стандарту зауваження та пропозиції, отримані під час громадського обговорення, враховано повністю.

Прийнято рішення проєкт Стандарту викласти у такій редакції:

ЗАТВЕРДЖЕНО
Наказом Міністерства
освіти і науки України

_____ 2023р. № _____

П Р О Е К Т

СТАНДАРТ ВИЩОЇ ОСВІТИ УКРАЇНИ

РІВЕНЬ ВИЩОЇ ОСВІТИ **Третій освітньо-науковий рівень**
(назва рівня вищої освіти)

СТУПІНЬ ВИЩОЇ ОСВІТИ **доктор філософії**
(назва ступеня вищої освіти)

ГАЛУЗЬ ЗНАНЬ **12 Інформаційні технології**
(шифр та назва галузі знань)

СПЕЦІАЛЬНІСТЬ **125 Кібербезпека та захист інформації**
(код та найменування спеціальності)

Видання офіційне

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Київ – 2023

I. Преамбула

Стандарт вищої освіти України (далі Стандарт) третій (освітньо-науковий) рівень, галузь знань 12 – Інформаційні технології, спеціальність 125 – Кібербезпека та захисті інформації.

Затверджено і введено в дію наказом Міністерства освіти і науки України від _____ 2023р. № _____.

Стандарт розроблено членами підкомісії зі спеціальності 125 – Кібербезпека Науково-методичної комісії № 7 з інформаційних технологій, автоматизації та телекомунікацій сектору вищої освіти Науково-методичної ради Міністерства освіти і науки України:

Юдін Олександр Костянтинівич – голова підкомісії 125 "Кібербезпека" науково-методичної комісії (НМК 7) з інформаційних технологій, автоматизації та телекомунікацій, доктор технічних наук, професор, Лауреат Державної премії України в галузі науки і техніки, завідувач спеціальної кафедри №31 Національної академії Служби безпеки України;

Кобозєва Алла Анатоліївна – заступник голови підкомісії, доктор технічних наук, професор, завідувач кафедри кібербезпеки та програмного забезпечення Одеського національного політехнічного університету;

Пархуць Любомир Теодорович – секретар підкомісії, доктор технічних наук, професор, заступник завідувача кафедри захисту інформації Національного університету "Львівська політехніка";

Бакалинський Олександр Олегович – член підкомісії, кандидат технічних наук, заступник директора Департаменту формування та реалізації державної політики у сфері кіберзахисту Адміністрації Державної служби спеціального зв'язку та захисту інформації України;

Васіліу Євген Вікторович – член підкомісії, доктор технічних наук, професор, директор Навчально-наукового інституту "Радіо, телебачення та інформаційної безпеки" Одеської національної академії зв'язку імені О.С.Попова;

Венгерський Петро Сергійович – член підкомісії, доктор фізико-математичних наук, завідувач кафедри кібербезпеки Львівського національного університету імені Івана Франка;

Євсєєв Сергій Петрович – член підкомісії, доктор технічних наук, професор, завідувач кафедри кібербезпеки Національного технічного університету "Харківський політехнічний інститут";

Чевардін Владислав Євгенійович – член підкомісії, доктор технічних наук, старший науковий співробітник, начальник кафедри кібербезпеки Військового інституту телекомунікацій та інформатизації імені Героїв Крут;

Халімов Геннадій Зайдулович – член підкомісії, доктор технічних наук, професор, завідувач кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки.

Стандарт розглянуто та схвалено на засіданні підкомісії зі спеціальності 125 – Кібербезпека Науково-методичної комісії № 7 з інформаційних технологій, автоматизації та телекомунікації Науково-методичної ради Міністерства освіти і науки України, протокол № ___ від _____ 2023 року.

Стандарт розглянуто на засіданні сектору вищої освіти Науково- методичної ради Міністерства освіти і науки України, протокол № ___ від _____ 2023 року.

Фахову експертизу проводили:

Методичну експертизу проводили:

Стандарт розглянуто

Стандарт розглянуто після надходження всіх зауважень і пропозицій та схвалено на засіданні підкомісії зі спеціальності зі спеціальності 125 – Кібербезпека Науково-методичної комісії № 7 з інформаційних технологій, автоматизації та телекомунікацій Науково-методичної ради Міністерства освіти і науки України, протокол № ___ від _____ 2023р.

Стандарт погоджено рішенням Національного агентства із забезпечення якості вищої освіти, протокол № ___ від _____ 2023 р.

II. Загальна характеристика

Рівень вищої освіти	Третій (освітньо-науковий) рівень
Ступінь вищої освіти	Доктор філософії
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Форми здобуття освіти	Очна (денна, вечірня), заочна
Освітня кваліфікація	Доктор філософії з кібербезпеки та захисту інформації
Професійна(і) кваліфікація(і)	
Кваліфікація в дипломі	Ступінь вищої освіти – Доктор філософії Галузь знань – 12 Інформаційні технології Спеціальність – 125 Кібербезпека та захист інформації
Опис предметної області	<p>Об'єкти вивчення та діяльності:</p> <ul style="list-style-type: none"> – проведення наукових досліджень, аналізу, створення та забезпечення функціонування інформаційних систем і технологій на об'єктах інформаційної діяльності та критичних інфраструктур сфери кібербезпеки та захисту інформації; – новітні системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – сучасні інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – автоматизовані системи управління інформаційною безпекою, кібербезпекою; – методології, технології, методи, моделі та засоби кібербезпеки та захисту інформації. <p>Цілі навчання: набуття здатності продукувати нові ідеї, розв'язувати комплексні проблеми в галузі професійної та дослідницько-інноваційної діяльності, а також здатності здійснювати науково-педагогічну діяльність у сфері кібербезпеки та захисту інформації, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики.</p> <p>Теоретичний зміст предметної області Принципи проведення наукових досліджень, теоретичні</p>

	<p>засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі кібербезпеки та захисту інформації.</p> <p>Методи, методики та технології</p> <p>Сучасні методи, моделі, методики та технології дослідження та вдосконалення процесів створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення наукових та професійних задач в галузі кібербезпеки та захисту інформації.</p> <p>Інструменти та обладнання.</p> <p>Програмно-апаратне та програмне забезпечення, інструментальні засоби, комп'ютерна техніка, спеціальні контрольні-вимірні прилади, програмно-технічні засоби автоматизації та системи автоматизації проектування, виробництва, експлуатації, контролю, моніторингу, мережні, мобільні, хмарні, технології, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків).</p>
Академічні права випускників	<p>Доктор філософії має право на здобуття наукового ступеня доктора наук та додаткових кваліфікацій у системі освіти дорослих.</p>
Працевлаштування випускників	<p>Працевлаштування на посадах наукових і науково-педагогічних працівників в наукових установах і закладах вищої освіти, посадах працівників найвищої кваліфікації у дослідницьких, проектних, конструкторських й т.п. установах і підрозділах підприємств.</p>

III. Вимоги до рівня освіти осіб, які можуть розпочати навчання за освітніми програмами відповідної спеціальності, та їх результатів навчання

Для здобуття освітньо-наукового ступеня доктора філософії зі спеціальності 125 Кібербезпека та захист інформації можуть вступати особи, які здобули освітній ступінь магістра. Програма фахових вступних випробувань для осіб, що здобули попередній рівень вищої освіти за іншими спеціальностями, повинна передбачати перевірку набуття особою компетентностей та результатів навчання, що визначені стандартом вищої освіти зі спеціальності 125 Кібербезпека та захист інформації для другого (магістерського) рівня вищої освіти.

IV. Обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти

Освітньо-наукова програма складається з освітньої та наукової складових. Нормативний строк підготовки доктора філософії в аспірантурі становить чотири роки. Обсяг освітньої складової освітньо-наукової програми підготовки доктора філософії становить 30-60 кредитів ЄКТС.

Наукова складова освітньо-наукової програми передбачає проведення власного наукового дослідження та оформлення його результатів у вигляді дисертації відповідно до законодавства.

V. Перелік компетентностей випускника

Інтегральна компетентність	Здатність продукувати нові ідеї, розв'язувати комплексні проблеми професійної та/або дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, застосовувати методологію наукової та педагогічної діяльності, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.
Загальні компетентності	ЗК-1. Здатність до абстрактного мислення, аналізу і синтезу. ЗК-2. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК-3. Здатність працювати в міжнародному контексті. ЗК-4. Здатність розв'язувати комплексні проблеми у сфері кібербезпеки та захисту інформації на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності.
Спеціальні	СК-1. Здатність виконувати оригінальні дослідження, досягати

(фахові, предметні) компетентності	наукових результатів, які створюють нові знання у сфері кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямках і можуть бути опубліковані у провідних наукових виданнях з кібербезпеки та захисту інформації.
	СК-2. Здатність ініціювати, розробляти і реалізовувати комплексні інноваційні проекти в сфері кібербезпеки та захисту інформації та дотичні міждисциплінарні проекти.
	СК-3. Здатність усно і письмово презентувати та обговорювати результати наукових досліджень та/або інноваційних розробок державною та іноземною мовами, глибоке розуміння наукових текстів в галузі кібербезпеки та захисту інформації.
	СК-4. Здатність здійснювати науково-педагогічну діяльність у вищій освіті. Здатність здійснювати професійну, наукову, науково-педагогічну діяльність у підприємствах, наукових установах і закладах вищої освіти.
	СК-5. Здатність ефективно застосовувати методи аналізу, математичне моделювання, виконувати натурні та обчислювальні експерименти при проведенні наукових досліджень у сфері кібербезпеки та захисту інформації.
	СК-6. Здатність інтегрувати знання з різних галузей, застосовувати системний підхід та враховувати нетехнічні аспекти при розв'язанні наукових задач та проведенні досліджень.
	СК-7. Здатність генерувати нові ідеї щодо розвитку теорії та практики кібербезпеки та захисту інформації, виявляти, ставити та вирішувати проблеми дослідницького характеру, оцінювати та забезпечувати якість виконуваних досліджень.

VI. Нормативний зміст підготовки здобувачів доктора філософії, сформульований у термінах результатів навчання

РН-1. Мати передові концептуальні та методологічні знання з кібербезпеки та захисту інформації і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з кібербезпеки та захисту інформації, ІТ-інфраструктур та інформаційних технологій, отримання нових знань та/або здійснення інновацій.
РН-2. Планувати і виконувати експериментальні та/або теоретичні дослідження з

<p>кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямів з використанням сучасних інструментів та дотриманням норм професійної і академічної етики, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблем.</p>
<p>РН-3. Глибоко розуміти загальні принципи та методи кібербезпеки та захисту інформації, а також методологію наукових досліджень, застосувати їх у власних дослідженнях у сфері інформаційних технологій та у викладацькій практиці.</p>
<p>РН-4. Розробляти та реалізовувати наукові та/або інноваційні інженерні проекти, які дають можливість переосмислити наявне та створити нове цілісне знання та/або професійну практику і розв'язувати значущі наукові та технологічні проблеми кібербезпеки та захисту інформації з дотриманням норм академічної етики і врахуванням соціальних, економічних, екологічних та правових аспектів.</p>
<p>РН-5. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані.</p>
<p>РН-6. Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми кібербезпеки та захисту інформації державною та іноземною мовами усно та письмово, оприлюднювати результати досліджень у наукових публікаціях у провідних вітчизняних та міжнародних наукових виданнях.</p>
<p>РН-7. Застосовувати загальні принципи та методи математики, інформатики та інших наук, а також сучасні методи та інструменти, цифрові технології та спеціалізоване програмне забезпечення для провадження наукових досліджень у сфері кібербезпеки та захисту інформації.</p>
<p>РН-8. Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямках.</p>
<p>РН-9. Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи.</p>
<p>РН-10. Організовувати і здійснювати освітній процес у сфері кібербезпеки та захисту інформації, його наукове, навчально-методичне та нормативне забезпечення, розробляти і викладати спеціальні навчальні дисципліни у закладах вищої освіти.</p>

VII. Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здобувачів освітнього рівня доктора філософії здійснюється у формі публічного захисту дисертації.
Вимоги до дисертації на здобуття ступеня доктора філософії	<p>Дисертація на здобуття ступеня доктора філософії є самостійним розгорнутим дослідженням, що пропонує розв'язання комплексної задачі в сфері кібербезпеки та захисту інформації, результати якого мають наукову новизну, теоретичне та практичне значення.</p> <p>Дисертація не повинна містити академічного плагіату, фальсифікації, фабрикації. Дисертація має бути розміщена на сайті закладу вищої освіти (наукової установи) (окрім робіт, які мають гриф обмеження доступу).</p>

VIII. Вимоги до створення міждисциплінарних освітньо-наукових програм

Для міждисциплінарних освітньо-наукових програм для зазначення спеціальності 125 Кібербезпека та захист інформації в освітній кваліфікації необхідно забезпечити набуття здобувачами третього (освітньо-наукового) рівня вищої освіти компетентностей ЗК-1, ЗК-4, СК-1, СК-3, СК-4, СК-6 та здобуття ними результатів навчання РН-1, РН-3, РН-4, РН-6, РН-7.

IX. Вимоги професійних стандартів у разі їх наявності

Повна назва та реквізити відповідного Професійного стандарту	Професійного стандарту немає
Особливості Стандарту вищої освіти, пов'язані з наявністю Професійного стандарту	

X. Додаткові вимоги до організації освітнього процесу для освітніх програм з підготовки фахівців для професій, для яких запроваджене додаткове регулювання

Додаткове регулювання не запроваджено

XI. Додаткові вимоги до структури освітніх програм, необхідних для доступу до професій, для яких запроваджене додаткове регулювання

Додаткове регулювання не запроваджено

ХІІ. Перелік нормативних документів, на яких базується стандарт вищої освіти

1. Закон "Про вищу освіту" – <http://zakon4.rada.gov.ua/laws/show/1556-18>.
2. Закон "Про освіту" – <http://zakon5.rada.gov.ua/laws/show/2145-19>.
3. Національна рамка кваліфікацій – <http://zakon4.rada.gov.ua/laws/show/13412011-п>.
4. Перелік галузей знань і спеціальностей, 2015 – <http://zakon4.rada.gov.ua/laws/show/266-2015-п>.
5. Постанова Кабінету Міністрів України "Про затвердження Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах) № 261 від 23 березня 2016 р. <https://zakon.rada.gov.ua/laws/show/261-2016-%D0%BF#Text>
6. Методичні рекомендації щодо розроблення стандартів вищої освіти, затверджені наказом Міністерства освіти і науки України від 01.06.2017 р. № 600 (у редакції наказу Міністерства освіти і науки України від 30.04.2020 р. № 584), схвалені сектором вищої освіти Науково-методичної Ради Міністерства освіти і науки України <https://mon.gov.ua/ua/osvita/visha-osvita/naukovo-metodichna-radaministerstva-osviti-i-nauki-ukrayini/metodichni-rekomendaciyi-vo>
7. Наказ Міністерства освіти і науки України "Про затвердження Вимог до міждисциплінарних освітніх (наукових) програм" № 128 від 01.02.2021 р. URL: <https://zakon.rada.gov.ua/laws/show/z0454-21#Text>
8. Стандарт вищої освіти за спеціальністю 125 "Кібербезпека" для першого (бакалаврського) рівня вищої освіти. URL: <https://mon.gov.ua/storage/app/media/vishcha-osvita/2022/Standarty.Vyshchoyi.Osvity/Zatverdzeni.Standarty/01/31/125-Kiberbezpeka-bak.31.01.22.pdf> .
9. Стандарт вищої освіти за спеціальністю 125 "Кібербезпека" для другого (магістерського) рівня вищої освіти. URL: [https://mon.gov.ua/storage/app/media/vyshcha/standarty/2021/03/19/125%20Kiberbezpeka mahistr 18 03 21 332.docx](https://mon.gov.ua/storage/app/media/vyshcha/standarty/2021/03/19/125%20Kiberbezpeka%20mahistr%2018%2003%2021%20332.docx) .

Генеральний директор директорату
фахової передвищої, вищої освіти

Олег ШАРОВ

Пояснювальна записка

Стандарт вищої освіти містить вимоги до освітніх програм підготовки докторів філософії за спеціальністю 125 Кібербезпека та захист інформації стосовно:

- обсягу освітніх програм для здобуття освітнього ступеня "доктор філософії" зі спеціальності 125 Кібербезпека та захист інформації;
- рівня освіти осіб, які можуть розпочати навчання за відповідною освітньою програмою;
- переліку обов'язкових компетентностей випускника;
- нормативного змісту підготовки здобувачів вищої освіти, сформульованого у термінах результатів навчання;
- форм атестації здобувачів вищої освіти;
- вимог до створення міждисциплінарних освітньо-наукових програм;

Вимоги до компетентностей та результатів навчання узгоджені між собою та відповідають дескрипторам Національної рамки кваліфікацій.

Таблиця 1 демонструє відповідність визначених Стандартом компетентностей та дескрипторів НРК, а таблиця 2 – відповідність результатів навчання та компетентностей.

Заклад вищої освіти самостійно визначає перелік дисциплін, практик та інших видів навчальної діяльності, необхідний для набуття означених Стандартом компетентностей та результатів навчання. Наведений в Стандарті перелік компетентностей і результатів навчання не є вичерпним. Заклади вищої освіти при формуванні освітніх програм можуть зазначати додаткові вимоги до компетентностей і результатів навчання. Заклади вищої освіти мають право використовувати власні формулювання спеціальних (фахових) компетентностей і результатів навчання, забезпечуючи при цьому, щоб сукупність вимог освітньої програми повністю охоплювала всі вимоги стандарту.

Працевлаштування випускників

Назви професій згідно Національного класифікатора України: Класифікатор професій (ДК 003:2010). Зазначений перелік не є вичерпним:

- 2310.2 – Викладач вищого навчального закладу (2310.2 Асистент)
- 2149.2 – Професіонал із організації інформаційної безпеки;
- 3439 – Інспектор з організації захисту секретної інформації;
- 1210.1 – Керівник підприємства (установи, організації) (сфера захисту інформації);
- 1226.2 – Керівник структурного підрозділу (сфера захисту інформації);
- 2433.1 – Науковий співробітник (інформаційна аналітика);
- 2433.1 – Науковий співробітник-консультант (інформаційна аналітика);

Рекомендовані джерела

1. The European Qualifications Framework: Supporting Learning, Work and Cross-Border Mobility.
URL: http://www.ehea.info/Upload/TPG_A_QF_RO_MK_1_EQF_Brochure.pdf.
2. QF-EHEA – Qualification Framework of the European Higher Education Area. URL: http://www.ehea.info/Upload/document/ministerial_declarations/EHEAParis2018_Co_m_munique_AppendixIII_952778.pdf.
3. Стандарти і рекомендації щодо забезпечення якості в Європейському просторі вищої освіти (ESG) – URL: https://ihed.org.ua/wpcontent/uploads/2018/10/04_2016_ESG_2015.pdf.
4. International Standard Classification of Education ISCED 2011 –
URL: <http://uis.unesco.org/sites/default/files/documents/international-standard-classificationof-education-isced-2011-en.pdf> .
5. International Standard Classification of Education: Fields of education and training 2013 (ISCED-F 2013) – URL: Detailed field descriptions –
<http://uis.unesco.org/sites/default/files/documents/international-standard-classificationof-education-fields-of-education-and-training-2013-detailed-field-descriptions-2015en.pdf> .
6. Manual to Accompany the International Standard Classification of Education 2011 –
URL: <http://uis.unesco.org/sites/default/files/documents/isced-fields-ofeducation-and-training-2013-en.pdf> .
7. Проект ЄС TUNING (прикладі результатів навчання, компетентностей)
<http://www.unideusto.org/tuningeu>.
8. Національний освітній глосарій: вища освіта / 2-е вид., перероб. і доп. / авт.-уклад. : В. М. Захарченко, С. А. Калашнікова, В. І. Луговий, А. В. Ставицький, Ю. М. Рашкевич, Ж. В. Таланова / За ред. В.Г.Кременя. – Київ : ТОВ "Видавничий дім "Плеяди", 2014. – 100 с. – URL: <http://erasmusplus.org.ua/korysna-informatsiia/korysni-materialy/category/3-materialynatsionalnoi-komandy-ekspertiv-shchodo-zaprovdzhennia-instrumentivbolonskohoprotsesu.html?download=83:hlosarii-terminiv-vyshchoi-osvity-2014-r-onovlenevydannia-z-urakhuvanniam-polozhen-novoho-zakonu-ukrainy-pro-vyshchuosvitu&start=80> .
9. Рашкевич Ю.М. Болонський процес та нова парадигма вищої освіти – URL: <http://erasmusplus.org.ua/korysna-informatsiia/korysni-materialy/category/3materialy-natsionalnoi-komandy-ekspertiv-shchodo-zaprovdzhennia-instrumentivbolonskohoprotsesu.html?download=82:bolonskyi-protses-nova-paradyhma-vyshchoiosvity-yu-rashkevych&start=80> .
10. Розвиток системи забезпечення якості вищої освіти в Україні: інформаційно-аналітичний огляд – URL: <http://erasmusplus.org.ua/korysnainformatsiia/korysni-materialy/category/3-materialy-natsionalnoi-komandy-ekspertivshchodo-zaprovdzhennia-instrumentivbolonskohoprotsesu.html?download=88:rozvytok-systemy-zabezpechennia-iakosti-vyshchoiosvity-ukrainy&start=80> .

11. Розроблення освітніх програм: методичні рекомендації / Авт.: В.М. Захарченко, В.І. Луговий, Ю.М. Рашкевич, Ж.В. Таланова / За ред. В.Г. Кременя. – Київ : ДП "НВЦ "Пріоритети", 2014. – 120 с. – URL: <http://erasmusplus.org.ua/korysna-informatsiia/korysni-materialy/category/3-materialynatsionalnoi-komandy-ekspertiv-shchodo-zaprovadzhennia-instrumentiv-bolonskohoprotsesu.html?download=84:rozroblennia-osvitnikh-prohram-metodychnirekomendatsii&start=80> .

**Матриця відповідності
визначених Стандартом компетентностей дескрипторам НРК**

Класифікація компетентностей за НРК	Знання Зн1. Концептуальні та методологічні знання в галузі чи на межі галузей знань або професійної діяльності.	Уміння/Навички Ум1. Спеціалізовані уміння/навички і методи, необхідні для розв'язання значущих задач у сфері професійної діяльності, науки та/або інновацій, розширення та переоцінки вже існуючих знань і професійної практики. Ум2. Започаткування, планування, реалізація та коригування послідовного процесу ґрунтового наукового дослідження з дотриманням належної академічної доброчесності. Ум3. Критичний аналіз, оцінка і синтез нових та комплексних ідей.	Комунікація К1. Вільне спілкування з питань, що стосуються сфери наукових та експертних знань, з колегами, широкою науковою спільнотою, суспільством в цілому. К2. Використання академічної державної та іноземної мови у професійній діяльності та дослідженнях.	Відповідальність і автономія АВ1. Демонстрація значної авторитетності, інноваційності, високий ступінь самостійності, академічна та професійна доброчесність, послідовна відданість розвитку нових ідей або процесів у передових контекстах професійної та наукової діяльності. АВ2. Здатність до безперервного саморозвитку та самовдосконалення.
	Загальні компетентності			
ЗК-1		Ум1		АВ1, АВ2
ЗК-2	Зн1	Ум1, Ум3	К2	АВ2
ЗК-3			К1, К2	АВ1, АВ2
ЗК-4	Зн1	Ум2	К2	АВ1, АВ2
Спеціальні (фахові) компетентності				
СК-1	Зн1	Ум1, Ум2, Ум3	К1, К2	АВ1, АВ2
СК-2			К1, К2	АВ1, АВ2
СК-3			К1	АВ2
СК-4	Зн1	Ум1, Ум2, Ум3		
СК-5	Зн1	Ум1, Ум2, Ум3		АВ2
СК-6		Ум2, Ум3	К1	АВ1
СК-7		Ум1, Ум2, Ум3		АВ2

**Матриця відповідності
визначених Стандартом результатів навчання та компетентностей**

Результати навчання	Компетентності										
	Інтегральна компетентність: Здатність розв'язувати комплексні проблеми в галузі професійної та/або дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики										
	Загальні компетентності				Спеціальні (фахові) компетентності						
	ЗК-1	ЗК-2	ЗК-3	ЗК-4	СК-1	СК-2	СК-3	СК-4	СК-5	СК-6	СК-7
РН-1			+		+					+	
РН-2	+	+		+	+	+	+			+	+
РН-3			+	+	+			+			
РН-4		+				+		+			+
РН-5	+			+		+					
РН-6	+		+		+		+		+	+	+
РН-7				+		+			+		
РН-8	+	+			+		+				+
РН-9	+	+	+					+	+		
РН-10	+		+					+			