МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАКАЗ

м. Київ

18 03 2021 р. № 332

Про затвердження стандарту
вищої освіти за спеціальністю
125 «Кібербезпека» для другого
(магістерського) рівня вищої освіти

На виконання частини шостої статті 10, підпункту 16 частини першої статті 13 Закону України «Про вищу освіту», підпункту 12 пункту 4 Положення про Міністерство освіти і науки України, затвердженого постановою Кабінету Міністрів України від 16 жовтня 2014 року № 630 з урахуванням Методичних рекомендацій щодо розроблення стандартів вищої освіти, затверджених наказом Міністерства освіти і науки України від 01червня 2016 року № 600 (в редакції наказу Міністерства освіти і науки України від 30 квітня 2020 року № 584),

НАКАЗУЮ:

1. Затвердити стандарт вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для другого (магістерського) рівня вищої освіти, що додається.
2. Установити, що стандарт вищої освіти, затверджений пунктом 1 цього наказу, вводиться в дію з 2021/2022 навчального року.
3. Контроль за виконанням цього наказу покласти на заступника Міністра з питань європейської інтеграції Вітренка А.

Міністр Сергій ШКАРЛЕТ

ЗАТВЕРДЖЕНО
Наказ Міністерства
освіти і науки України

18.03.2021 р. № 332

СТАНДАРТ ВИЩОЇ ОСВІТИ УКРАЇНИ

РІВЕНЬ ВИЩОЇ ОСВІТИ **ДРУГИЙ (МАГІСТЕРСЬКИЙ) РІВЕНЬ**
(назва рівня вищої освіти)

СТУПІНЬ ВИЩОЇ ОСВІТИ **МАГІСТР**
(назва ступеня вищої освіти)

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

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

Видання офіційне

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Київ – 2021

І. Преамбула

Стандарт вищої освіти України: другий (магістерський) рівень, галузь знань 12 Інформаційні технології, спеціальність 125 Кібербезпека.

Затверджено і введено в дію наказом Міністерства освіти і науки України від 18.03.2021 р. № 332.

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 Костянтинович – 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.

Василіу Євген Вікторович – член підкомісії, доктор технічних наук, професор, декан факультету кібербезпеки, комп'ютерних і радіо технологій" Державного університету інтелектуальних технологій і зв'язку.

Венгерський Петро Сергійович – член підкомісії, доктор фізико-математичних наук, професор кафедри інформаційних систем Львівського національного університету імені Івана Франка.

Євсеєв Сергій Петрович – член підкомісії, доктор технічних наук, професор, завідувач кафедри кібербезпеки та інформаційних технологій Харківського національного економічного університету імені Семена Кузнеця.

Чевардін Владислав Євгенійович – член підкомісії, доктор технічних наук, старший науковий співробітник, начальник кафедри захисту інформації та кіберзахисту 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.

Фахівці, залучені до розроблення стандарту:

Івченко Ірина Сергіївна – Віце-президент Громадської організації «ІСАКА КИЇВ», ISACA Kyiv Chapter.

Стандарт розглянуто на засіданні сектору вищої освіти Науково- методичної ради Міністерства освіти і науки України від 26.05.2020 року, протокол № 1.

Фахову експертизу проводили:

Мачуський Євгеній Андрійович – доктор технічних наук, професор, заслужений діяч науки і техніки України, завідувач кафедри засобів захисту інформації фізико-технічного інституту Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

Горбенко Іван Дмитрович – доктор технічних наук, професор, Лауреат Державної премії України в галузі науки й техніки, відмінник освіти України, професор кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В.Н. Каразина.

Баранік Володимир Вікторович – доктор технічних наук, професор, начальник кафедри бойового застосування та експлуатації автоматизованих систем управління Харківського національного університету Повітряних Сил ім. І. Кожедуба.

Коляденко Владимир Адольфович – кандидат технічних наук, Голова Комітету з електронних комунікацій Торгово-Промислової Палати України.

Методичну експертизу проводили:

Рашкевич Юрій Михайлович, доктор технічних наук, професор, член Національного агентства кваліфікацій, Національний експерт Програми ЄС Еразмус+.

Таланова Жаннета Василівна, доктор педагогічних наук, с.н.с., доцент; г.н.с. Інституту вищої освіти НАПН України; менеджер з аналітичної роботи Національного Еразмус+ офісу в Україні.

Стандарт схвалено Державною службою спеціального зв’язку та захисту інформації України та Федерацією роботодавців України.

Стандарт розглянуто після надходження всіх зауважень і пропозицій та схвалено на засіданні підкомісії зі спеціальності 125 "Кібербезпека" Науково-методичної комісії № 7 з інформаційних технологій, автоматизації та телекомунікацій Науково-методичної ради Міністерства освіти і науки України, протокол № 4 від 05.02.2021 р.

Стандарт погоджено рішенням Національного агентства із забезпечення якості вищої освіти, протокол від 23.02.2021 р. № 3.

ІІ. Загальна характеристика

Рівень вищої освіти	Другій рівень
Ступінь, що присвоюється	Магістр
Назва галузі знань	12 Інформаційні технології
Назва спеціальності	125 Кібербезпека
Форми здобуття освіти	Денна, заочна, дистанційна, дуальна
Освітня кваліфікація	Магістр з кібербезпеки за спеціалізацією (зазначити назву спеціалізації за наявності)
Кваліфікація в дипломі	Ступінь вищої освіти – Магістр Спеціальність – 125 Кібербезпека Спеціалізація – (назва спеціалізації за наявності)
Опис предметної області	**Об'єкти вивчення:** – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; – інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. **Цілі навчання:** Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки.

	Теоретичний зміст предметної області Теоретичні 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 інформаційної безпеки та/або кібербезпеки. **Методи, методики та технології** Методи, моделі, методики та технології 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 професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. **Інструменти та обладнання**. Засоби, пристрої, 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 інформаційної безпеки та/або кібербезпеки.
Академічні права випускників	Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.

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

Для здобуття освітнього рівня магістра можуть вступати особи, що здобули освітній рівень бакалавра.

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 для першого (бакалаврського) рівня вищої освіти.

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

Обсяг освітньої програми магістра:

освітньо-професійної програми – 90 кредитів ЄКТС;

освітньо-наукової програми – 120 кредитів ЄКТС.

Мінімум 60% обсягу освітньої програми має бути спрямовано на формування загальних та спеціальних (фахових) компетентностей за спеціальністю, визначених Стандартом вищої освіти.

Освітньо-наукова програма магістра обов'язково включає дослідницьку (наукову) компоненту обсягом не менше 30%.

Мінімум 15 кредитів ЄКТС має бути призначено для практики.

Заклад вищої освіти має право визнати та перезарахувати кредити ЄКТС, отримані за попередньою освітньою програмою підготовки магістра (спеціаліста) за іншою спеціальністю. Максимальний обсяг кредитів ЄКТС, що може бути перезарахований, становить 25% від загального обсягу освітньої програми.

V. Перелік компетентностей випускника

Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності	КЗ-1. Здатність застосовувати знання у практичних ситуаціях. КЗ-2. Здатність проводити дослідження на відповідному рівні. КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Фахові компетентності	КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

	КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки. **Додатково для освітньо-наукових програм** КФ11. Здатність здійснювати наукові та/або прикладні дослідження у галузі інформаційної безпеки та/або кібербезпеки із застосуванням сучасних експериментальних і теоретичних методів моделювання процесів, формувати науково-технічну звітність

VI. Нормативний зміст підготовки здобувачів вищої освіти, сформульований у контексті результатів навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку

ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури.

РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об’єктивно оцінювати результати навчання.

РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

РН21. Використовувати методи натурного, фізичного і комп’ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

Додатково для освітньо-наукових програм

РН24. Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики.

РН25. Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.

VII. Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Кваліфікаційна робота має бути розміщена на офіційному сайті (або у репозитарії) закладу вищої освіти або його підрозділу. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

VIII. Вимоги до створення освітніх програм підготовки за галуззю знань або групою спеціальностей міждисциплінарних освітньо-наукових програм

Для міждисциплінарних освітньо-наукових програм для зазначення спеціальності 125 Кібербезпека в освітній кваліфікації необхідно забезпечити набуття здобувачами другого (магістерського) рівня вищої освіти загальних компетентностей КЗ-1–КЗ-3, КЗ-5, спеціальних компетентностей КФ1–КФ4, КФ6, КФ8, КФ10, КФ11 та результатів навчання РН1, РН2, РН4, РН5, РН7– РН9, РН11, РН13, РН15–РН18, РН20, РН21, РН23–РН25.

IX. Вимоги професійних стандартів у разі їх наявності

Повна назва та реквізити відповідного Професійного стандарту	
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

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

– Закон України "Про вищу освіту" – http://zakon4.rada.gov.ua/laws/show/1556-18.
– Закон України "Про освіту" – http://zakon5.rada.gov.ua/laws/show/2145-19.

– Національний класифікатор України: "Класифікатор професій" ДК 003:2010.
– Національна рамка кваліфікацій – https://zakon.rada.gov.ua/laws/show/1341-2011-%D0%BF#Text.
– Перелік галузей знань і спеціальностей – http://zakon4.rada.gov.ua/laws/show/266-2015-п.
– Методичні рекомендації щодо розроблення стандартів вищої освіти. Затверджено 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 – https://mon.gov.ua/storage/app/media/vyshcha/naukovo-metodychna_rada/2020metod-rekomendacziyi.docx

IX. Перелік рекомендованих джерел

1. Стандарти та рекомендації щодо забезпечення якості в Європейському просторі вищої освіти (ESG) // URL: https://ihed.org.ua/wpcontent/uploads/2018/10/04_2016_ESG_2015.pdf.
2. EQF 2017 (Європейська рамка кваліфікацій) // URL: https://ec.europa.eu/ploteus/sites/eac-eqf/files/en.pdf; https://ec.europa.eu/ploteus/content/descriptors-page.
3. QF EHEA 2018 (Рамка кваліфікацій ЄПВО) // URL: http://www.ehea.info/Upload/document/ministerial_declarations/EHEAParis2018_Communique_AppendixIII_952778.pdf
4. ISCED (Міжнародна стандартна класифікація освіти, МСКО) 2011 // URL: http://uis.unesco.org/sites/default/files/documents/international-standardclassification-of-education-isced-2011-en.pdf.
5. ISCED-F (Міжнародна стандартна класифікація освіти – Галузі, МСКО-Г) 2013 // URL: http://uis.unesco.org/sites/default/files/documents/internationalstandard-classification-of-education-fields-of-education-and-training-2013-detailedfield-descriptions-2015-en.pdf.
6. TUNING (для ознайомлення зі спеціальними (фаховими) та загальними компетентностями та прикладами стандартів – http://www.unideusto/ org/tuningeu/.
7. 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.– К. : ТОВ "Видавничий дім "Плеяди", 2014.– 100 с. – http://erasmusplus.org.ua/korysnainformatsiia/korysni-materialy/category/3-materialy-natsionalnoi-komandyekspertiv-shchodo-zaprovadzhennia-instrumentiv-bolonskohoprotsesu.html?download=83:hlosarii-terminiv-vyshchoi-osvity-2014-r-onovlenevydannia-z-urakhuvanniam-polozhen-novoho-zakonu-ukrainy-pro-vyshchuosvitu&start=80.
8. Рашкевич Ю.М. Болонський процес та нова парадигма вищої освіти – http://erasmusplus.org.ua/korysna-informatsiia/korysni-materialy/category/3 materialy-natsionalnoi-komandy-ekspertiv-shchodo-zaprovadzhennia-instrumentivbolonskoho-protsesu.html?download=82:bolonskyi-protses-nova-paradyhmavyshchoi-osvity-yu-rashkevych&start=80.
9. Розвиток системи забезпечення якості вищої освіти в Україні: інформаційно-аналітичний огляд – http://erasmusplus.org.ua/korysna-

informatsiia/korysni-materialy/category/3-materialy-natsionalnoi-komandy-ekspertiv-shchodozaprovadzhennia-instrumentiv-bolonskoho-protsesu.html?download=88:rozvytoksystemy-zabezpechennia-iakosti-vyshchoi-osvity-ukrainy&start=80.
10. Розроблення освітніх програм: методичні рекомендації / Авт.: В.М. Захарченко, В.І. Луговий, Ю.М. Рашкевич, Ж.В. Таланова / За ред. В.Г. Кременя. – К. ДП "НВЦ "Пріоритети", 2014. – 120 с. – http://erasmusplus.org.ua/korysna-informatsiia/korysni-materialy/category/3-materialy-natsionalnoikomandy-ekspertiv-shchodo-zaprovadzhennia-instrumentiv-bolonskohoprotsesu.html?download=84:rozroblennia-osvitnikh-prohram-metodychnirekomendatsii&start=80.

Генеральний директор директорату
фахової передвищої, вищої освіти Олег ШАРОВ

ПОЯСНЮВАЛЬНА ЗАПИСКА

до стандарту вищої освіти України другого ступеня вищої освіти – магістр, галузі знань – 12 "Інформаційні технології", спеціальності – 125 "Кібербезпека"

Стандарт вищої освіти містить вимоги до освітніх програм підготовки магістрів за спеціальністю 125 "Кібербезпека" стосовно:

– обсягу кредитів ЄКТС, необхідного для здобуття освітнього ступеня "магістр" зі спеціальності 125 "Кібербезпека";

– рівня освіти осіб, які можуть розпочати навчання за відповідною освітньою програмою, та результатів їх навчання;

– 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 (НРК).

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 освітніх компонентів, необхідних для набуття передбачених 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.

Заклад вищої освіти має право запроваджувати додаткові форми атестації здобувачів вищої освіти.

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.

Таблиця 1

Матриця відповідності визначених Стандартом компетентностей / результатів навчання дескрипторам НРК

Класифікація компетентностей (результатів навчання) за НРК	**Знання** **Зн1** Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем у галузі та на межі галузей знань	**Уміння/Навички Ум1** Спеціалізовані уміння/навички розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур **Ум2** Здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах **Ум3** Здатність розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності	**Комунікація К1** Зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і нефахівців, зокрема до осіб, які навчаються	**Відповідальність і автономія АВ1** Управління робочими або навчальними процесами, які є складними, непередбачуваними та потребують нових стратегічних підходів **АВ2** Відповідальність за внесок до професійних знань і практики та/або оцінювання результатів діяльності команд та колективів **АВ3** Здатність продовжувати навчання з високим ступенем автономії
Загальні компетентності				
КЗ1	Зн1,	Ум1, Ум3	К1	АВ1, АВ2
КЗ2	Зн1,	Ум1, Ум2, Ум3		АВ2, АВ3
КЗ3	Зн1	Ум2, Ум3		АВ1
КЗ4	Зн1	Ум3		АВ1, АВ2
КЗ5	Зн1	Ум2	К1	АВ1
Спеціальні (фахові) компетентності				
КФ1	Зн1	Ум2		АВ2
КФ2	Зн1,	Ум2		АВ2
КФ3	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2
КФ4	Зн1,	Ум1, Ум2	К1	АВ1, АВ2
КФ5	Зн1,	Ум1, Ум2	К1	АВ1, АВ2
КФ6	Зн1	Ум1, Ум2	К1	АВ1
КФ7	Зн1	Ум1, Ум2	К1	АВ1
КФ8	Зн1	Ум1, Ум2	К1	АВ1
КФ9	Зн1	Ум1, Ум2	К1	АВ1
КФ10	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2
Додатково для освітньо-наукових програм*				
КФ11*	Зн1,	Ум1, Ум2, Ум3		АВ2, АВ3

Таблиця 2

відності визначених Стандартом результатів навчання та компетентностей

Програмні результати навчання	Компетентності															
	Інтегральна компетентність															
	Загальні компетентності					Спеціальні (фахові) компетентності										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	Кф-5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ11*
РН 1	+		+			+										
РН 2		+	+			+	+	+								+
РН 3	+					+										+
РН 4	+	+	+	+		+	+									
РН 5			+		+		+									+
РН 6	+			+		+		+		+	+	+		+		
РН 7	+		+				+									
РН 8	+	+		+	+			+						+	+	
РН 9	+	+	+	+					+					+	+	
РН 10	+		+	+						+				+		
РН 11	+		+	+							+				+	
РН 12	+		+	+					+			+			+	
РН 13	+		+	+									+		+	
РН 14	+		+	+					+					+	+	
РН 15				+	+										+	
РН 16	+	+	+	+				+	+	+	+	+		+	+	+
РН 17								+							+	
РН 18	+			+	+										+	
РН 19	+			+	+	+	+	+	+		+	+	+	+		
РН 20	+	+	+	+	+	+		+								+
РН 21	+	+	+	+		+		+		+		+	+			+
РН 22		+	+	+		+		+								+
РН 23	+		+	+		+	+	+			+	+	+	+		
Додатково для освітньо-наукових програм*																
РН 24*		+	+	+	+			+							+	+
РН 25*	+	+	+	+				+								+