МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАКАЗ

29 10 2024 **м. Київ** № 1547

Про внесення змін до стандарту вищої освіти зі спеціальності 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти

Відповідно до частини шостої статті 10, пункту 16 частини першої статті 13 Закону України «Про вищу освіту», постанови Кабінету Міністрів України від 29 квітня 2015 року № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» (зі змінами), підпункту 12 пункту 4 Положення про Міністерство освіти і науки України, затвердженого постановою Кабінету Міністрів України від 16 жовтня 2014 року № 630 (зі змінами), наказу Міністерства освіти і науки України від 05 квітня 2023 року № 392 «Про особливості запровадження змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, затверджених постановою Кабінету Міністрів України від 16 грудня 2022 року №1392», зареєстрованого в Міністерстві юстиції України 12 травня 2023 року за № 806/39862, з урахуванням Методичних рекомендацій щодо розроблення стандартів вищої освіти, затверджених наказом Міністерства освіти і науки України від 01.06.2016 № 600 (у редакції наказу Міністерства освіти і науки України від 30.04.2020 № 584), погодження Національного агентства із забезпечення якості вищої освіти від 22 жовтня 2024 року (протокол № 18 (68)

НАКАЗУЮ:

1. Внести зміни до стандарту вищої освіти зі спеціальності 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для першого (бакалаврського) рівня вищої освіти, затвердженого наказом Міністерства освіти і науки України від 04.10.2018 № 1074 (далі стандарт вищої освіти), виклавши його у новій редакції, що додається.

2. Установити, що стандарт вищої освіти вводиться в дію з 2024/2025 навчального року.

3. Департаменту забезпечення документообігу, контролю та інформаційних технологій (Єрко І.) зробити відповідну відмітку у справах архіву.

4. Контроль за виконанням цього наказу покласти на заступника Міністра Винницького М.

Міністр **Оксен ЛІСОВИЙ**

ЗАТВЕРДЖЕНО
Наказ Міністерства освіти і науки України
04.10.2018 № 1074
(у редакції наказу Міністерства освіти і науки України
29 10 2024 № 1547)

СТАНДАРТ ВИЩОЇ ОСВІТИ

РІВЕНЬ ВИЩОЇ ОСВІТИ **Перший (бакалаврський)**
(назва рівня вищої освіти)

СТУПІНЬ ВИЩОЇ ОСВІТИ **бакалавр**
(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 – 2024

І Преамбула

Стандарт вищої освіти України (далі – Стандарт), перший (бакалаврський) рівень, галузь знань 12 Інформаційні технології, спеціальність 125 Кібербезпека та захист інформації.

Затверджено і введено в дію наказом Міністерства освіти і науки України від 29 10 2024 № 1547.

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, доктор технічних наук, професор, Лауреат Державної премії України в галузі науки і техніки, учений секретар Державного науково-дослідного інституту технологій кібербезпеки;

Кобозєва Алла Анатоліївна – заступник голови підкомісії, доктор технічних наук, професор, професор кафедри технічної кібернетики й інформаційних технологій ім. професора Р. В. Мерката Одеського національного морського 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, старший дослідник, заступник директора Департаменту європейської інтеграції та міжнародного співробітництва Адміністрації Державної служби спеціального зв'язку та захисту інформації України;

Василіу Євген Вікторович – член підкомісії, доктор технічних наук, професор, в. о. декана факультету «Інформаційних технологій та кібербезпеки» Державного університету інтелектуальних технологій і зв'язку;

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

Євсеєв 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 № 6 від 07.12.2023.

Стандарт розглянуто на засіданні сектору вищої освіти Науково-методичної ради Міністерства освіти і науки України.

Фахову експертизу проводили:

Хорошко Володимир Олексійович – доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету;

Нємкова Олена Анатоліївна – доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій Національного університету «Львівська політехніка»;

Толюпа Сергій Васильович – доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Методичну експертизу проводили:

Бахрушин Володимир Євгенович, доктор фізико-математичних наук, професор, професор кафедри системного аналізу та обчислювальної математики Національного університету «Запорізька політехніка»;

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 розглянуто Державною службою спеціального зв'язку та захисту інформації України і 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 № 3 від 05.09.2024.

Стандарт погоджено рішенням Національного агентства із забезпечення якості вищої освіти, протокол № 18 (68) від 22.10.2024.

ІІ Загальна характеристика

Рівень вищої освіти	Перший (бакалаврський) рівень
Ступінь, що присвоюється	Бакалавр
Назва галузі знань	12 Інформаційні технології
Назва спеціальності	125 Кібербезпека та захист інформації
Форми здобуття освіти	Денна, заочна, дуальна
Освітня кваліфікація	Бакалавр з кібербезпеки та захисту інформації
Професійна кваліфікація	–
Кваліфікація в дипломі	Ступінь вищої освіти – Бакалавр Спеціальність – 125 Кібербезпека та захист інформації Освітня програма – (зазначити назву)
Додаткові вимоги до правил прийому	–
Опис предметної області	**Об'єкти вивчення**: – технології кібербезпеки та захисту інформації; – процеси управління кібербезпекою та захистом інформації; об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології. **Цілі навчання:** підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації. **Теоретичний зміст предметної області**: Принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. **Методи, методики та технології:** методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації. **Інструменти та обладнання**: засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне

	забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).
Академічні права випускників	Мають право на здобуття освіти на другому (магістерському) рівні вищої освіти. Здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.
Працевлаштування випускників	На посади у структурних підрозділах установ/ підприємств/організацій, які передбачають наявність вищої освіти зі спеціальності 125 Кібербезпека та захист інформації.

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

Для здобуття освітнього ступеня бакалавра зі спеціальності 125 Кібербезпека та захист інформації можуть вступати особи, які здобули повну загальну середню освіту.

Прийом на основі здобутого ступеня молодшого бакалавра, фахового молодшого бакалавра або освітньо-кваліфікаційного рівня молодшого спеціаліста здійснюється в порядку, визначеному законодавством.

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

Обсяг кредитів ЄКТС, необхідний для здобуття ступеня бакалавра зі спеціальності 125 Кібербезпека та захист інформації становить:

- на базі повної загальної середньої освіти – 240 кредитів ЄКТС;
- на базі здобутих освітніх ступенів молодшого бакалавра, фахового молодшого бакалавра (освітньо-кваліфікаційного рівня молодшого спеціаліста) заклад вищої освіти має право визнати та перезарахувати не більше ніж 60 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки фахівців.

Мінімум 50% обсягу освітньої програми має бути спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю, визначених цим Стандартом вищої освіти.

V Перелік компетентностей випускника:

Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності	**ЗК1**. Здатність застосовувати знання у практичних ситуаціях **ЗК2**. Знання та розуміння предметної області і розуміння професійної діяльності **ЗК 3.** Здатність спілкуватися державною мовою як усно, так і письмово. **ЗК 4.** Здатність спілкуватися іноземною мовою. **ЗК 5**.. Здатність вчитися і оволодівати сучасними знаннями.

	ЗК 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні. **ЗК 7**. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. **ЗК 8**. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Спеціальні (фахові, предметні) компетентності	**СК1**. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.
	СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.
	СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.
	СК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.
	СК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.
	СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)
	СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.
	СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
	СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.
	СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й

	інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

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

РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.

РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.

РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.

РН14. Вирішувати задачі управління процесами відновлення штатного

функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації. **РН15**. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи. **РН16**. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах; **РН17**. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. **РН18**. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. **РН19**. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. **РН20**. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. **РН21**. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

VII Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту. Заклади вищої освіти мають право встановлювати додаткові форми атестації
Вимоги до єдиного державного кваліфікаційного іспиту	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених цим стандартом.
Вимоги до кваліфікаційної роботи (за наявності)	Кваліфікаційна робота має передбачати розв'язок спеціалізованого завдання теоретичного або практичного спрямування в галузі кібербезпеки та захисту інформації. У кваліфікаційній роботі не повинно бути академічного плагіату, фальсифікації та фабрикації. Кваліфікаційна робота має бути оприлюднена (за виключенням робіт, що містять інформацію з обмеженим

	доступом) на офіційному сайті закладу вищої освіти або його структурного підрозділу, або у репозитарії закладу вищої освіти.

VIII Вимоги до створення освітніх програм підготовки за галуззю знань, двома галузями знань, міждисциплінарних освітньо-професійних програм

Створення міждисциплінарних освітніх програм на бакалаврському рівні не передбачено.

IX Вимоги професійних стандартів у разі їх наявності

Повна назва та реквізити відповідного Професійного стандарту	1. Адміністратор безпеки мереж і систем, 2139.2 2. Фахівець сфери захисту інформації, 2139.2 3. Фахівець з питань безпеки (інформаційно-комунікаційні технології), 2139.2 4. Конструктор систем кібербезпеки, 2132.2 5. Фахівець з підтримки інфраструктури кіберзахисту, 2139.2 6. Фахівець з реагування на інциденти кібербезпеки, 2139.2 7. Фахівець з криптографічного захисту інформації, 2139.2 8. Фахівець з технічного захисту інформації, 2139.2 9. Фахівець з тестування систем захисту інформації, 2139.2 10.Аудитор інформаційних технологій (з кібербезпеки), 2139.2 11.Фахівець з оцінки заходів захисту інформації (кібербезпеки), 2139.2
Особливості Стандарту вищої освіти, пов'язані з наявністю Професійного стандарту	У стандарті вищої освіти враховані основні цілі професійної діяльності відповідно до наявних професійних стандартів (Додаток 4)

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

1. Про вищу освіту: Закон України. URL: http://zakon4.rada.gov.ua/laws/show/1556-18.

2. Про освіту: Закон України. URL: http://zakon5.rada.gov.ua/laws/show/2145-19.

3. Закон України «Про захист персональних даних». URL: https://zakon.rada.gov.ua/laws/show/2297-17.

4. Закон України «Про доступ до публічної інформації» https://zakon.rada.gov.ua/laws/show/2939-17.

5. Закон України «Про основні засади забезпечення кібербезпеки України» https://zakon.rada.gov.ua/laws/show/2163-19.

6. Закон України «Про захист інформації в інформаційно-комунікаційних системах» https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

7. Закон України «Про державну таємницю». https://zakon.rada.gov.ua/laws/show/3855-12.

8. Закон України «Про науково-технічну інформацію». https://zakon.rada.gov.ua/laws/show/3322-12.

9. Постанова Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури». https://zakon.rada.gov.ua/laws/show/518-2019-п

10. Національний класифікатор України: Класифікатор професій ДК 003:2010 (із змінами). URL: https://zakon.rada.gov.ua/rada/show/va327609-10.

11. Постанова Кабінету Міністрів України від 23 листопада 2011 р. №1341 (із змінами) «Про затвердження Національної рамки кваліфікацій» URL: http://zakon4.rada.gov.ua/laws/show/1341-2011-п.

12. Постанова Кабінету Міністрів України від 29 квітня 2015 р. № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти». URL: http://zakon4.rada.gov.ua/laws/show/266-2015-п.

13. Постанова Кабінету Міністрів України від 16 грудня 2022 р. № 1392 «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти». URL: https://www.kmu.gov.ua/npas/pro-vnesennia-zmin-do-pereliku-haluzei-znan-i-spetsialnostei-za-iakymy-zdiisniuietsia-pidhotovka-zdobuvachiv-vyshchoi-osvity-i161222-1392.

14. Наказ 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) «Про затвердження Методичних рекомендацій щодо розроблення стандартів вищої освіти». URL: https://mon.gov.ua/storage/app/media/vyshcha/naukovometodychna_rada/2020-metod-rekomendacziyi.docx.

Генеральний директор директорату фахової передвищої, вищої освіти **Олег ШАРОВ**

ПОЯСНЮВАЛЬНА ЗАПИСКА

Стандарт вищої освіти містить вимоги до освітньо-професійних програм підготовки бакалаврів за спеціальністю 125 Кібербезпека та захист інформації стосовно:

– обсягу освітньо-професійних програм для здобуття бакалаврського ступеня вищої освіти зі спеціальності 125 Кібербезпека та захист інформації;

– переліку обов'язкових компетентностей випускника;

– нормативного змісту підготовки здобувачів вищої освіти, сформульованого у термінах результатів навчання;

– форм атестації здобувачів вищої освіти.

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

В Додатках 1,2,3 наведено відповідність фахових компетентностей та програмних результатів навчання, програмних результатів навчання та компетентностей, відповідність компетентностей дескрипторам НРК; в Додатку 4 наведено перелік Професійних стандартів з зазначенням мети діяльності за професією.

Заклад вищої освіти самостійно визначає перелік освітніх компонентів, форм організації освітнього процесу, видів навчальних занять, необхідних для задоволення визначених Стандартом вимог. 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 з урахуванням обмежень, визначених цим стандартом.

Враховуючи автономність закладу вищої освіти, додатковою формою атестації може бути кваліфікаційна робота. Рішення про введення додаткової форми атестації приймається вченою радою ЗВО. Кваліфікаційна робота (за наявності) має передбачати розв'язок спеціалізованого завдання теоретичного та/або практичного спрямування в галузі кібербезпеки та захисту інформації. У кваліфікаційній роботі не має бути академічного плагіату, фальсифікації та фабрикації. Кваліфікаційна робота має бути оприлюднена (за виключенням робіт, що містять інформацію з обмеженим доступом) на офіційному сайті закладу вищої освіти або його структурного підрозділу, або у репозитарії закладу вищої освіти.

Рекомендовані джерела

1. International Standard ClassificationofEducation (ISCED 2011). https://www.datenportal.bmbf.de/portal/en/G294.html#:~:text=ISCED%20was%20developed%20by%20UNESCO,facilitating%20national%20and%20international%20comparisons.

2. ISCED FieldsofEducationandTraining 2013 (ISCED-F 2013).: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://uis.unesco.org/sites/default/files/documents/isced-fields-of-education-and-training-2013-en.pdf;

3. TheEuropeanQualificationsFramework: SupportingLearning, WorkandCrossBorderMobility. URL: http://www.ehea.info/Upload/TPG_A_QF_RO_MK_1_EQF_Brochure.pdf;

4. QF-EHEA – QualificationFrameworkoftheEuropeanHigherEducationArea.;

5. Стандарти та рекомендації щодо забезпечення якості в Європейському просторі вищої освіти (ESG). Режим доступу: https://ihed.org.ua/wp-content/uploads/2018/10/04_2016_ESG_2015.pdf;

6. HigherEducationintheWorld 8 - Specialissue. NewVisionsforHigherEducationtowards 2030. Barcelona, GUNi, May 2022. URL: https://www.guninetwork.org/files/guni_heiw_8_complete_-_new_visions_for_higher_education_towards_2030_1.pdf

7. TUNING EducationalStructuresinEurope (Проєкт Європейської Комісії "Налаштування освітніх систем в Європі (для ознайомлення з прикладами стандартів та вимог до компетентностей для різних предметних областей) http://www.ehea.info/cid101886/tuning-educational-structures-europe.html .

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. – Режим доступу: http://onu.edu.ua/pub/bank/userfiles/files/nauk%20method%20rada/glossariy.pdf

9. Бахрушин В.Є. Стандартизація вимог до вищої освіти, як інструмент забезпечення якості вищої освіти: рівні вищої освіти та предметні області. Освітня аналітика України. 2020. № 2(9). С. 50–66. URL: https://science.iea.gov.ua/wp-content/uploads/2020/10/4_Bakhrushin_29_2020_50_66.pdf .

10. Рашкевич Ю.М. Болонський процес: історія, стан та перспективи. Освітня аналітика України 2018, № 3 (4), С. 5–16 – URL: https://science.iea.gov.ua/wp-content/uploads/2018/12/5_16_Rashkevich.pdf

11. Розвиток системи забезпечення якості вищої освіти в Україні: інформаційно-аналітичний огляд – URL: https://lib.iitta.gov.ua/9412/1/%D0%A0%D0%BE%D0%B7%D0%B2%D0%B8%D1%82%D0%BE%D0%BA_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B8_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF_%D1%8F%D0%BA%D0%BE%D1%81%D1%82%D0%B8.pdf

12. 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: https://core.ac.uk/download/pdf/32308651.pdf

Додаток 1

Зведена таблиця фахових компетентностей та програмних результатів навчання

Фахові компетентності	Результати навчання
СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації	РН9. Вміти застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації
СК2. Здатність до використання інформаційних технологій, сучасних методів і моделей кібербезпеки та систем захисту інформації.	РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.	РН11. Планувати підготовку та забезпечувати неперервність процесів в організаціях згідно встановленої політики кібербезпеки та з урахування вимог до захисту інформації.
СК4. Здатність забезпечувати захист інформації в інформаційних системах згідно встановленої політики кібербезпеки та захисту інформації	РН12. Застосовувати методи захисту інформації в інформаційних системах згідно встановленої політики інформаційної безпеки. РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних та програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних систем та\або інфраструктури організації в цілому.;
СК5. Здатність відновлювати функціонування інформаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.	РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних систем з використанням процедур резервування згідно встановленої політики безпеки та забезпечувати функціонування спеціального програмного забезпечення, щодо захисту та відновлення інформації; РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації	РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах;

(комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо)	
СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою	РН17. Забезпечувати функціонування системи управління кібербезпекою та захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності	РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.	РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування та контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.
СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти та оцінювати можливі вразливості та загрози інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.	РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору та інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

Додаток 2

Матриця відповідності визначених Стандартом результатів навчання та компетентностей

Результати навчання	Компетентності																				
		Загальні компетентності								Спеціальні (фахові) компетентності											
	Інтегральна компетентність	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
РН1	+			+															
РН2	+				+														
РН3	+						+	+											
РН4	+	+	+																
РН5	+	+	+																
РН6	+		+						+										
РН7	+	+							+										
РН8	+					+													
РН9	+						+			+									
РН10	+										+								
РН11	+											+							
РН12	+												+						
РН13	+												+						
РН14	+													+					
РН15	+													+					
РН16	+														+				
РН17	+															+			
РН18	+																+		
РН19	+																+		
РН20	+																	+	
РН21	+																		+

Додаток 3

Матриця відповідності визначених Стандартом компетентностей дескрипторам НРК

Класифікація компетентностей (результатів навчання) за НРК	**Знання** **Зн1** Концептуальні наукові та практичні знання. **Зн2** Критичне осмислення теорій, принципів, методів і понять у сфері професійної діяльності та/або навчання.	**Уміння** **Ум1.** Поглиблені когнітивні та практичні уміння/навички, майстерність та інноваційність на рівні, необхідному для розв'язання складних спеціалізованих задач і практичних проблем у сфері професійної діяльності або навчання.	**Комунікація** **К1.** Донесення до фахівців і нефахівців інформації, ідей, проблем, рішень, власного досвіду та аргументації. **К2.** Збір, інтерпретація та застосування даних. **К3.** Спілкування з професійних питань, у тому числі іноземною мовою, усно та письмово.	**Відповідальність та автономія** **АВ1.** Управління складною технічною або професійною діяльністю чи проектами. **АВ2.** Спроможність нести відповідальність за вироблення та ухвалення рішень у непередбачуваних робочих та/або навчальних контекстах. **АВ3.** Формування суджень, що враховують соціальні, наукові та етичні аспекти. **АВ4.** Організація та керівництво професійним розвитком осіб та груп. **АВ5.** Здатність продовжувати навчання із значним ступенем автономії.
ЗК1	**Зн2**	**Ум1**		
ЗК2	**Зн2**	**Ум1**	**К1**	
ЗК3			**К1, К3**	
ЗК4			**К1, К3**	
ЗК5	**Зн1, Зн2**	**Ум1**	**К2**	**АВ3**
ЗК6	**Зн1**		**К1**	**АВ2, АВ3, АВ4**
ЗК7			**К1**	**АВ2**
ЗК8	**Зн2**		**К2**	**АВ3**
СК1	**Зн2**	**Ум1**	**К2**	
СК2	**Зн1, Зн2**	**Ум1**	**К2**	
СК3		**Ум1**		**АВ1**
СК4		**Ум1**		**АВ1**
СК5		**Ум1**	**К2**	**АВ1, АВ2**
СК6		**Ум1**	**К1**	**АВ1**
СК7		**Ум1**	**К1**	**АВ1**
СК8	**Зн2**	**Ум1**		
СК9	**Зн2**	**Ум1**		
СК10		**Ум1**	**К2**	**АВ2**

Додаток 4

Перелік професійних стандартів

№	Назва професійного стандартута код згідно з Національним класифікатором України ДК 003:2010 «Класифікатор професій»	Мета діяльності за професією
	Адміністратор безпеки мереж і систем, 2139.2	Встановлення та підтримка мереж і систем, їх конкретних компонентів (встановлення, конфігурування і оновлення апаратного та програмного забезпечення, обслуговування баз даних, створення та управління обліковими записами користувачів, нагляд або виконання резервного копіювання та відновлення, впровадження оперативного та технічного контролів безпеки; дотримання політик та процедур безпеки організації тощо). Адміністрування системи управління даними, що дозволяють безпечно зберігати, обробляти, запитувати, захищати та використовувати дані.
	Фахівець сфери захисту інформації, 2139.2	Забезпечення захищеності (конфіденційності, цілісності, доступності) інформації, що обробляється (передається) в інформаційних (автоматизованих), електронних комунікаційних та інформаційно-комунікаційних системах від несанкціонованих дій з інформацією (включаючи комп'ютерні віруси), від витоку технічними каналами та від спеціальних впливів на засоби обробки інформації, а також інформації, що озвучується на об'єктах інформаційної діяльності, – від витоку технічними каналами.
	Фахівець з питань безпеки (інформаційно-комунікаційні технології), 2139.2	Організація та забезпечення кібербезпеки інформаційних систем та інформаційно-комунікаційних технологій; управління наслідками реалізації загроз інформаційної безпеки в межах організації, в тому числі управління спеціальними програмами (проектами) інших сфер відповідальності; формування стратегічного розвитку організації, персоналу, інфраструктури, вимог до безпеки, а також розробка та впровадження політики та стратегії інформаційної безпеки інституції; планування заходів безпеки інформації та кіберзахисту на випадок надзвичайних ситуацій або при реалізації інцидентів; обізнаність про безпеку інформаційних ресурсів організації або анклаву, установ та підприємств різних форм власності.
	Конструктор систем кібербезпеки, 2132.2	Забезпечення ситуації, коли вимоги безпеки зацікавлених сторін, необхідні для захисту місії організації та бізнес-процесів, належним чином ураховуються в усіх аспектах архітектури систем кібербезпеки організації (установи, підприємства), включаючи еталонні моделі, архітектури сегментів та рішень, а також системи для підтримки цих місій та бізнес-процесів.
	Фахівець з підтримки інфраструктури кіберзахисту, 2139.2	Тестування, впровадження, розгортання, підтримка та адміністрування інфраструктурного обладнання та програмного забезпечення кіберзахисту
	Фахівець з реагування на інциденти кібербезпеки, 2139.2	Аналіз, оцінка інцидентів кібербезпеки в рамках мережевого середовища та реагування на них. Усунення інцидентів кібербезпеки та пом'якшення їх наслідків. Відстеження, оцінка стану кібербезпеки систем та своєчасне повідомлення про інциденти кібербезпеки. Відновлення функціональності систем і процесів до робочого стану. Дослідження та аналіз заходів реагування, оцінка ефективності та покращення існуючих практик. Накопичення та проведення аналізу даних про кіберзагрози.
	Фахівець з криптографічного захисту інформації, 2139.2	Забезпечення криптографічного захисту інформації в інформаційних системах\мережах (або автоматизованих системах, інформаційно-комунікаційних системах, системах електронних комунікацій) на основі перетворень інформації з використанням спеціальних даних (ключових даних) для приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

		Здійснення оцінки рівня безпеки та контролю стану криптографічного захисту інформації в інформаційних системах\мережах (або автоматизованих системах, інформаційно-комунікаційних системах, системах електронних комунікацій). Дослідження рівня захисту програмних засобів і систем що реалізують криптографічні функції. Супроводження робіт зі створення, впровадження та забезпечення функціонування підсистем криптографічного захисту інформації на всіх етапах життєвого циклу інформаційних систем\мереж в організаціях, підприємствах або установах різних форм власності.
	Фахівець з технічного захисту інформації, 2139.2	Забезпечення інженерно-технічними та організаційно-технічними заходами та засобами порядку доступу, конфіденційності, цілісності й доступності (унеможливлення блокування) інформації, яка становить державну та іншу передбачену законом таємницю, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави. Захист інформації та безпосередньо її властивостей, спрямований на забезпечення за допомогою нормативно-правових, організаційних та інженерно-технічних заходів та/або програмно-технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації. Супроводження робіт зі створення, впровадження та забезпечення функціонування систем технічного захисту інформації на етапах життєвого циклу інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем (далі – автоматизовані системи).
	Фахівець з тестування систем захисту інформації, 2139.2	Планування, підготовка та проведення тестування або тестування на проникнення до інформаційних систем/мереж (або автоматизованих систем, інформаційно-комунікаційних систем, систем електронних комунікацій), а також їх інформаційних ресурсів (активів або компонентів) в організаціях, підприємствах або установах різних форм власності. Проведення оцінки стану захищеності інформаційних систем/мереж та стану кібербезпеки на відповідність стандартам, специфікаціям, нормам, вимогам та заявленим технічним характеристикам. Проведення аналізу й звітування щодо результатів тестування, розроблення рекомендацій з виявлення та оцінки відхилень у функціонуванні операційних процесів, а також звітування щодо визначених вразливостей і загроз інформаційній системі та її ресурсам.
	Аудитор інформаційних технологій (з кібербезпеки), 2139.2	Проведення внутрішнього та зовнішнього аудиту об'єктів інформатизації для надання об'єктивних якісних і кількісних оцінок про поточний стан інформаційної безпеки організації у відповідності з визначеними в нормативно-правовій, нормативно-технічний базі критеріями та показниками безпеки. Формування рекомендацій, на основі наданих оцінок, для посилення системи менеджменту інформаційної безпеки, підтримки планів стійкості, відновлення штатного функціонування інфраструктури організації після інцидентів та нештатних ситуацій.
	Фахівець з оцінки заходів захисту інформації (кібербезпеки), 2139.2	Здійснення незалежної комплексної оцінки управлінського, операційного та технічного контролю безпеки, а також покращення контролю, що використовується в системі інформаційних технологій для визначення загальної ефективності заходів контролю. Розроблення, забезпечення та контроль виконання заходів для усунення причин і умов, що можуть призвести до витоку інформації. Здійснення оцінки ступеню захищеності інформаційних систем, а також системного контролю реалізації задекларованих послуг безпеки. Підвищення рівня безпеки інформаційних систем на основі аналізу потенційних недоліків та вразливих точок, а також забезпечення економічної ефективності розгорнутих заходів захисту.
	Кібероператор, 4113	Здійснення збору та оброблення чутливої інформації (даних) та/або встановлення і аналіз геолокації інформаційних систем/мереж для експлуатації, пошуку та/або відстеження цілей (інформаційних потоків або об'єктів), що являють інтерес для інституції, організації, чи установи різних форм власності в рамках чинного законодавства. Виконання мережевої навігації, збирання даних відповідного спрямування з відкритих джерел за допомогою різних онлайн-інструментів, виконання тактичного криміналістичного аналізу, а також у випадку поставленої задачі, в рамках чинного законодавства, прийняття участі у виконанні операцій в інформаційній системі/мережі.