МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАКАЗ

04 10 2018 р. **м. Київ** № 1044

Про затвердження стандарту
вищої освіти за спеціальністю
125 «Кібербезпека» для першого
(бакалаврського) рівня вищої освіти

Відповідно до частини шостої статті 10, підпункту 16 частини першої статті 13 Закону України «Про вищу освіту» та рішення Колегії Міністерства освіти і науки України від 24.04.2018 р., протокол № 4/3-4,

НАКАЗУЮ:

1. Затвердити стандарт вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для першого (бакалаврського) рівня вищої освіти, що додається.
2. Установити, що затверджений стандарт вищої освіти вводиться в дію з 2018/2019 навчального року.
3. Контроль за виконанням цього наказу покласти на заступника Міністра Рашкевича Ю. М.

Міністр Л. М. Гриневич

Наказ Міністерства
освіти і науки України

04.10.2018 р. № 1074

СТАНДАРТ ВИЩОЇ ОСВІТИ УКРАЇНИ

перший (бакалаврський) рівень
(назва рівня вищої освіти)

бакалавр
(назва ступеня, що присвоюється)

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
2018

І. Преамбула

Стандарт вищої освіти України: перший (бакалаврський) рівень, галузь знань 12 – Інформаційні технології, спеціальність 125 – Кібербезпека

Затверджено і введено в дію наказом Міністерства освіти і науки України від 04.10.2018 р. № 1047

Стандарт розроблено членами підкомісії зі спеціальності 125 – Кібербезпека Науково-методичної комісії № 8 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 8) з інформаційних технологій, автоматизації та телекомунікацій, директор Навчально-наукового інституту комп'ютерних інформаційних технологій Національного авіаційного університету.

Оксіюк Олександр Глібович – заступник голови підкомісії 125 «Кібербезпека» науково-методичної комісії (НМК 8) з інформаційних технологій, автоматизації та телекомунікацій, завідувач кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка;

Бабенко Тетяна Василівна – завідувач кафедри безпеки інформації та телекомунікацій Державного вищого навчального закладу «Національний гірничий університет»;

Бурячок Володимир Леонідович – провідний науковий співробітник кафедри інформаційних технологій і математичних дисциплін Київського університету імені Бориса Грінченка;

Воронов Віктор Романович – заступник начальника управління Департаменту технічного захисту інформації Адміністрації Державної служби спеціального зв'язку та захисту інформації України;

Качинський Анатолій Броніславович – професор кафедри інформаційної безпеки Національного технічного університету України "Київський політехнічний інститут";

Кузнєцов Олександр Олександрович – професор кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна;

Максимович Володимир Миколайович – завідувач кафедри безпеки інформаційних технологій Національного університету «Львівська політехніка»;

Чечельницький Віктор Якович – директор Інституту інформаційної безпеки, радіоелектроніки Одеського національного політехнічного університету.

Стандарт розглянуто та схвалено на засіданні підкомісії зі спеціальності 125 – Кібербезпека Науково-методичної комісії № 8 з інформаційних

технологій, автоматизації та телекомунікацій Науково-методичної ради Міністерства освіти і науки України 25.05.2016 р. протокол № 2.

Стандарт розглянуто на засіданні сектору вищої освіти Науково-методичної ради Міністерства освіти і науки України від 27 вересня 2016 року, протокол №7.

Фахову експертизу проводили:

Чаузов Олександр Миколайович, перший заступник Голови Державної служби спеціального зв'язку та захисту інформації України,

Василіу Євген Вікторович, директор науково-навчального інституту Одеської національної академії зв'язку ім. О.С. Попова,

Іллічов Руслан Володимирович, Генеральний директор Федерації роботодавців України,

Капля Ігор Ігоревич, директор ТОВ «БМС Консалтинг»,

Лисицький Ігор Вікторович, Голова Всеукраїнської громадської організації «Рада з конкурентоспроможності індустрії інформаційно-комунікаційних технологій України».

Методичну експертизу проводили:

Калашнікова Світлана Андріївна, доктор педагогічних наук, професор, директор Інституту вищої освіти НАПН України;

Таланова Жаннета Василівна, доктор педагогічних наук, доцент, старший науковий співробітник, менеджер з аналітичної роботи Національного Еразмус+ офісу в Україні.

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

Стандарт розглянуто після надходження всіх зауважень та пропозицій та схвалено на засіданні підкомісії зі спеціальності зі спеціальності 125 – Кібербезпека Науково-методичної комісії № 8 з інформаційних технологій, автоматизації та телекомунікацій Науково-методичної ради Міністерства освіти і науки України 14.06.2017 протокол № 4

ІІ. Загальна характеристика

Рівень вищої освіти	Перший (бакалаврський) рівень
Ступінь, що присвоюється	Бакалавр
Назва галузі знань	12 Інформаційні технології
Назва спеціальності	125 Кібербезпека
Обмеження щодо форм навчання	Денна, заочна, дистанційна
Освітня кваліфікація,	бакалавр з кібербезпеки
Кваліфікація в дипломі	Ступінь вищої освіти – Бакалавр Спеціальність – 125 Кібербезпека Спеціалізація – (зазначити назву спеціалізації за наявності) Освітня програма – (зазначити назву)
Опис предметної області	Об’єкти професійної діяльності випускників: – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту. Цілі навчання підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. Теоретичний зміст предметної області Знання – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного

	захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування. Методи, методики та технології: Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки. Інструменти та обладнання: – системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Академічні права випускників	Можливість продовжити навчання за освітньою програмою ступеня магістра.

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

Обсяг освітньої програми бакалавра:

- на базі повної загальної середньої освіти– 240 кредитів ЄКТС

- на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») заклад вищої освіти має право визнати та перезарахувати не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста).

Мінімум 75% обсягу освітньої програми має бути спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю визначеною стандартом вищої освіти.

IV. Перелік компетентностей випускника

Інтегральна компетентність	Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності	КЗ 1. Здатність застосовувати знання у практичних ситуаціях.
	КЗ 2. Знання та розуміння предметної області та розуміння професії.
	КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
	КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

	КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.
	КЗ 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 і свобод людини і громадянина в Україні;
	КЗ 7. 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.
Фахові компетентності	КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
	КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
	КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
	КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
	КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
	К 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.
	КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
	КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
	КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною

	та/або кібербезпекою.
	КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.
	КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
	КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

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

Кінцеві, підсумкові та інтегративні результати навчання, що визначають нормативний зміст підготовки і корелюються з визначеним вище переліком загальних і спеціальних компетентностей, подано нижче.

	Результати навчання
1.	- застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
2.	- організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
3.	- використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
4.	- аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;
5.	- адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;
6.	- критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;
7.	- діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;
8.	- готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;
9.	- впроваджувати процеси, що базуються на національних та міжнародних

	стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
10.	- виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;
11.	- виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах;
12.	- розробляти моделі загроз та порушника;
13.	- аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;
14.	- вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;
15.	- використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;
16.	- реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;
17.	- забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;
18.	- використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;
19.	- застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
20.	- забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;
21.	- вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
22.	- вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;
23.	- реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
24.	- вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних

	(автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);
25.	- забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;
26.	- впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;
27.	- вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
28.	- аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки;
29.	- здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;
30.	- здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
31.	- застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
32.	- вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;
33.	- вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;
34.	- приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;
35.	- вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;
36.	- виявляти небезпечні сигнали технічних засобів;
37.	- вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;

38.	- інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;
39.	- проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;
40.	- інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;
41.	- забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;
42.	- впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;
43.	- застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;
44.	- вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;
45.	- застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;
46.	- здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;
47.	- вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;
48.	- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;
49.	- забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;
50.	- забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);
51.	- підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;
52.	- використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;
53.	- вирішувати задачі аналізу програмного коду на наявність можливих

	загроз.
54.	- усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

VI. Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту кваліфікаційного проекту/роботи та за рішенням закладу вищої освіти кваліфікаційного екзамену. На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання за даним стандартом. До атестації допускаються студенти, які виконали всі вимоги програми підготовки.
Вимоги до кваліфікаційної роботи/проекту	Кваліфікаційний проект/робота має передбачати розв'язання спеціалізованої задачі в галузі інформаційної та/або кібербезпеки. Кваліфікаційний проект/ робота має бути перевірений на плагіат. Оприлюднення на сайті.

VII. Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

У закладі вищої освіти повинна функціонувати система забезпечення закладом вищої освіти якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості), яка передбачає здійснення таких процедур і заходів:

1) визначення принципів та процедур забезпечення якості вищої освіти;

2) здійснення моніторингу та періодичного перегляду освітніх програм;

3) щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників закладу вищої освіти та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті закладу вищої освіти, на інформаційних стендах та в будь-який інший спосіб;

4) забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників;

5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за кожною освітньою програмою чи спеціальністю;

6) забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;

7) забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації;

8) забезпечення ефективної системи запобігання та виявлення академічного плагіату у наукових працях працівників закладів вищої освіти і здобувачів вищої освіти;

9) інших процедур і заходів.

Система забезпечення закладом вищої освіти якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості) за поданням ВНЗ оцінюється Національним агентством із забезпечення якості вищої освіти або акредитованими ним незалежними установами оцінювання та забезпечення якості вищої освіти на предмет її відповідності вимогам до системи забезпечення якості вищої освіти, що затверджуються Національним агентством із забезпечення якості вищої освіти, та міжнародним стандартам і рекомендаціям щодо забезпечення якості вищої освіти.

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

1. Закон України «Про вищу освіту» 01.07.2014 №1556-VII - Режим доступу: http://zakon4.rada.gov.ua/laws/show/1556-18.
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» - відомості Верховної Ради України (ВВР), 1994, N 31, ст.286
3. Закон України "Про основні засади забезпечення кібербезпеки України"- відомості Верховної Ради (ВВР), 2017, № 45, ст.403;
4. «Доктрина інформаційної безпеки України», затверджено Указом Президента України від 25 лютого 2017 року № 47/2017.
5. Постанова Кабінету Міністрів «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 29.04.2015 р. № 266
6. Рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» від 27.01.2016 р., уведеного в дію Указом Президента України від 15.03.2016 р. № 96.
7. Постанова Кабінету Міністрів «Про затвердження Ліцензійних умов провадження освітньої діяльності» від 30.12.2015 № 1187Наказ МОН України №166 «Деякі питання оприлюднення інформації про діяльність вищих навчальних закладів» від 19.02.2015 р.
8. Наказ МОН України «Про особливості запровадження переліку галузей знань, за якими здійснюється підготовка здобувачів вищої освіти, затвердженого постановою Кабінету Міністрів України від 29.04. 2015 р.» № 266 від 06.11.2015 р. №1151.
9. Національний класифікатор України: "Класифікатор професій" ДК 003:2010 // Видавництво "Соцінформ". - К.: 2010
10. Наказ Міністерства економічного розвитку і торгівлі України від «Про затвердження зміни до національного класифікатора України ДК 003:2010» від 18.11. 2014 р. № 1361 (зміна № 2)
11. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27 вересня 1999 р. № 1229;

12. Положення про порядок здійснення криптографічного захисту інформації в Україні, затверджене Указом Президента України від 22 травня 1998 р. № 505;
13. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29 березня 2006 р. № 373.

Генеральний директор директорату
вищої освіти і освіти дорослих О. І. Шаров

Додаток №1

Зведена таблиця фахових компетентностей та результатів навчання.

Фахові компетентності	Результати навчання
КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.	- готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки; - розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем; - виконувати аналіз реалізації прийнятої політики інформаційної і /або кібербезпеки.
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.	- здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; -розробляти та аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; -застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур операційних систем; -здійснювати захист ресурсів і процесів в інформаційно-телекомунікаційних системах на основі моделей безпеки (кінцевих автоматів, управління потоками, *Bell-LaPadula, Biba, Clark-Wilson*, та інші), а також встановлених режимів безпечного функціонування інформаційно-телекомунікаційних системах; - виконувати аналіз програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної і\або кібербезпеки в інформаційно-телекомунікаційних системах.
КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах	-забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; - забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - виконувати розробку експлуатаційної документації на комплексів засобів захисту.
КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.	- вирішувати задачі супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - вирішувати задачі управління доступом до інформаційних

	ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); - вирішувати задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - забезпечувати введення підзвітності системи управління доступом інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
КФ 5 Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	- обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної та/або кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації; - вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах - проектувати та реалізувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації; -вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; -використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.	-вирішувати задачі управління процесами забезпечення безперервності бізнесу з використанням процедур резервування програмного забезпечення та безпосередньо інформаційних ресурсів; -вирішувати задачі корекції цілей, стратегій, планів забезпечення безперервності бізнес процесів після здійснення кібератак, збоїв та відмов різних класів. -створювати і впроваджувати плани процесу забезпечення безперервності бізнесу; - виконувати аналіз налаштувань елементів інформаційних систем та комунікаційного обладнання;
КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів	- вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; -здійснювати оцінку рівня захищеності інформації що обробляється в інформаційно-телекомунікаційних системах використовувати інструментальні засоби оцінювання

та ін.)	наявності потенційних вразливостей; - вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих); - вирішувати задачі експертизи, випробування комплексних систем захисту інформації.
КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.	- вирішувати задачі попередження та виявлення, ідентифікації, аналізу та реагування на інциденти в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - проводити розслідування інцидентів інформаційної безпеки та/або кібербезпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної безпеки та/або кібербезпеки; - забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації;
КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.	- забезпечувати безперервність бізнес процесів організації на базі теорії ризиків та системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів; -забезпечувати функціонування системи управління інформаційною та\або кібербезпекою організації на основі керування інформаційними ризиками, здійснення процедур їх кількісного і якісного оцінки;
КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.	- аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації; - аналізувати та визначати можливість застосування технологій, методів та засобів технічного захисту інформації; - виявляти небезпечні сигнали технічних засобів; - вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю захищеності інформації від витоку технічними каналами; - визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; - інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; – обґрунтовувати можливість створення технічних каналів витоку інформації на об’єктах інформаційної діяльності; – впроваджувати заходи та засоби технічного захисту інформації від витоку технічними каналами;
КФ 11. Здатність виконувати моніторинг ресурсів і процесів функціонування, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики	- забезпечувати процеси моніторингу доступу до ресурсів і процесів інформаційно-телекомунікаційних систем; -забезпечувати конфігурування та функціонування систем моніторингу ресурсів та процесів в інформаційно-телекомунікаційних системах;

інформаційної та/або кібербезпеки.	
КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно встановленої політики інформаційної та/або кібербезпеки.	- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в інформаційно-телекомунікаційних системах; - аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.

Додаток №2

Додаткова література.

1. Payment Card Industry Data Security Standard (PCI DSS ISO/IEC 27001:2013).
2. ISO/IEC 27002:2012/16 Information technology. Security techniques. Code of practice for information security management – Інфорацій1ні технології. Стандарт.
3. ISO/IEC 27005:2011 Information security risk management — Управління ризиками інформаційної безпеки. Стандарт.
4. ISO/IEC 27032:2016 Information technology. «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности».
5. International Standard Classification of Occupations 2008, міжнародний класифікатор професій.
6. Розвиток системи забезпечення якості вищої освіти в Україні: інформаційно-аналітичний огляд, Національна академія педагогічних наук України, Інститут вищої освіти НАПН України, Режим доступу: http://ihed.org.ua/images/biblioteka/Rozvitok_sisitemi_zabesp_yakosti_VO_UA_2015.pdf
7. Розроблення освітніх програм: методичні рекомендації - Режим доступу: http://ihed.org.ua/images/biblioteka/rozroblennya_osv_program_2014_tempus-office.pdf
8. Методичні рекомендації щодо розроблення стандартів вищої освіти.
9. Bragg R. Certified Information Systems Security Professional (CISSP, International Standard).
10. Stewart J. M. SSCP Systems Security Certified Practitioner. – 2006.
11. CobiT C. Control Objectives for Information and related Technology //IT Governance Institute www. isaca. org. – 2002.
12. Information technology–Security techniques–Information security management systems–Requirements. – 2005.
13. Commissie E. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. – 2013.
14. Індустріальної моделі Кібербезпеки США - 3.2-2016, ETA USD: Cybersecurity Industry Model:2014. International Standard.

15. «Біла книга Держспецзв'язку», Електронний ресурс. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=49942&cat_id=49941
16. TUNING (для ознайомлення зі спеціальними (фаховими) компетентностями та прикладами стандартів - http://www.unideusto.org/tuningeu.