

ГАЛУЗЕВИЙ СТАНДАРТ ВИЩОЇ ОСВІТИ УКРАЇНИ

ПОГОДЖЕНО
Перший заступник Міністра
освіти і науки України
Суліма Є.М.
« » 20 р.



ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ПІДГОТОВКИ магістра

ГАЛУЗИ ЗНАНЬ	1701 “Інформаційна безпека”
НАПРЯМ ПІДГОТОВКИ	6.170101 “Безпека інформаційних і комунікаційних систем”
СПЕЦІАЛЬНІСТЬ	8.17010102 “Безпека державних інформаційних ресурсів”
КВАЛІФІКАЦІЯ	2149.2 "Професіонал із організації захисту інформації з обмеженим доступом "

Видання офіційне

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Київ

2013

**ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми**

Освітньо-кваліфікаційний рівень

магістр

Галузь знань

1701 "Інформаційна безпека"

Напрямок підготовки

6.170101 "Безпека інформаційних і комунікаційних систем"

Спеціальність

8.17010102 "Безпека державних інформаційних ресурсів"

Кваліфікація

2149.2 "Професіонал із організації захисту інформації з обмеженим доступом"

**Міністерство освіти і науки, молоді та спорту України
"ПОГОДЖЕНО"**

Департамент вищої освіти



(підпис) _____ (прізвище та ініціали)
" " 20__ р.

Інститут інноваційних технологій і змісту освіти



(підпис) _____ (прізвище та ініціали)
" " 20__ р.

М.П. Голова НМК/підкомісії



(підпис) О.М.Новіков
(прізвище та ініціали)
" " 20__ р.


Співголова НМК/підкомісії



(підпис) О.К.Юдін
(прізвище та ініціали)
" " 20__ р.

Керівник закладу-розробника
Ректор Національного авіаційного університету

Керівник розробки



(підпис) М.С.Кулик
" " 20__ р.

д.т.н., професор, завідувач спеціальної кафедри №1 _____
(науковий ступінь та вчене звання, посада)

Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут"

М.П. 

(підпис) Скрипник Л.В.
(прізвище та ініціали)
" " 03 20__ р.

РОЗРОБЛЕНО Робочою групою Міністерства освіти і науки, молоді та спорту України

ВНЕСЕНО Національним авіаційним університетом

ЗАТВЕРДЖЕНО ТА НАДАНО ЧИННОСТІ
Наказом Міністерства освіти і науки, молоді та спорту України
від 25.07.2013 р. №1039

ВВЕДЕНО ВПЕРШЕ

РОЗРОБНИКИ СТАНДАРТУ

Скрипник Леонід Васильович, заслужений діяч науки і техніки України, лауреат державної премії України в галузі науки і техніки, доктор технічних наук, професор, завідувач спеціальної кафедри №1 Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут".

Горбенко Іван Дмитрович, доктор технічних наук, професор, завідувач кафедри "Безпеки інформаційних технологій" Харківського національного університету радіоелектроніки".

Проскуровський Роман Васильович, кандидат технічних наук, заступник завідувача спеціальної кафедри №1 Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут".

Конюшок Сергій Миколайович, кандидат технічних наук, доцент, заступник начальника Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут" з навчальної та наукової роботи.

Заболотний Володимир Ілліч, кандидат технічних наук, доцент, професор кафедри "Безпеки інформаційних технологій" Харківського національного університету радіоелектроніки".

Зміст

Вступ	4
1. Галузь використання	5
2. Нормативні посилання	6
3. Визначення	6
4. Позначення і скорочення	6
5. Розподіл змісту освітньо-професійної програми та максимальний навчальний час за циклами підготовки	6
6. Нормативна частина змісту освітньо-професійної програми	6
7. Державна атестація осіб, які навчаються у вищих навчальних закладах	7
8. Вимоги до системи освіти та професійної підготовки	7
Додаток А Розподіл змісту освітньо-професійної програми та максимальний навчальний час за циклами підготовки	9
Додаток Б Система змістових модулів.....	10
Додаток В Перелік навчальних дисциплін і практик та система блоків змістових модулів	16
Додаток Г Розподіл змісту освітньо-професійної програми підготовки, навчальний час за циклами підготовки, навчальними дисциплінами й практиками та перелік сформованих компетенцій.....	19
Додаток Д Нормативні форми державної атестації.....	20

Вступ

Освітньо-професійна програма (ОПП) є галузевим нормативним документом, у якому визначається нормативний термін та зміст навчання, встановлюються вимоги до змісту, обсягу і рівня освіти та професійної підготовки фахівця зі спеціальності 8.17010102 "Безпека державних інформаційних ресурсів".

Цей стандарт використовується при:

- розробці та корегуванні складової галузевих стандартів вищої освіти (засобів діагностики якості вищої освіти);

- розробці та корегуванні складових стандартів вищої освіти вищих навчальних закладів (варіативної частини освітньо-професійної програми підготовки та засобів діагностики якості вищої освіти, навчального плану, програм навчальних дисциплін і практик тощо);

- визначенні змісту навчання в системі перепідготовки та підвищення кваліфікації фахівців.

1 Галузь використання

Цей стандарт поширюється на систему вищої освіти: органи, які здійснюють управління у галузі вищої освіти; інші юридичні особи, що надають освітні послуги у галузі вищої освіти; вищі навчальні заклади всіх форм власності, де готують фахівців:

освітньо-кваліфікаційного рівня	магістр
галузі знань	1701 "Інформаційна безпека"
за спеціальністю	8.17010102 "Безпека державних інформаційних ресурсів"
освітнього рівня	повна вища освіта
кваліфікації	2149.2 "Професіонал із організації захисту інформації з обмеженим доступом"
з узагальненим об'єктом діяльності	методи, засоби, системи і технології захисту державних інформаційно-телекомунікаційних систем, системи урядового зв'язку і Національної системи конфіденційного зв'язку, державних інформаційних ресурсів, криптографічного та технічного захисту інформації

Цей стандарт встановлює:

- нормативну частину змісту навчання, засвоєння якої забезпечує формування системи умінь відповідно до вимог освітньо-професійної характеристики;
- рекомендований перелік навчальних дисциплін і практик;
- нормативний термін навчання за денною формою навчання;
- нормативні форми державної атестації.

Стандарт є обов'язковим для вищих навчальних закладів, що готують фахівців цього профілю. Підприємства, установи, організації мають забезпечити необхідні умови для використання фахівців відповідно до здобутих ними у вищому навчальному закладі кваліфікації та спеціальності згідно чинного законодавства.

Стандарт можна використовувати під час проведення ліцензування та акредитації вищих навчальних закладів, атестації осіб, які закінчили навчання у вищих навчальних закладах, та сертифікації фахівців.

2 Нормативні посилання

В цьому стандарті використані посилання на нормативні документи:

- ГСВОУ 6.170101-10 "Галузевий стандарт вищої освіти України. Освітньо-кваліфікаційна характеристика".
- ГСВОУ 6.170101-10 "Галузевий стандарт вищої освіти України. Освітньо-професійна програма".
- ГСВОУ 8.17010102-12 "Галузевий стандарт вищої освіти України. Освітньо-кваліфікаційна характеристика".

3 Визначення

ГСВОУ 8.17010102-12 "Галузевий стандарт вищої освіти України. Освітньо-кваліфікаційна характеристика".

4 Позначення та скорочення

У даному нормативному документі для формування шифрів застосовуються скорочення назв, що наведені у ГСВОУ ОПП 6.170101-10.

5 Розподіл змісту освітньо-професійної програми та максимальний навчальний час за циклами підготовки

Освітньо-професійна програма передбачає такі цикли підготовки:

- гуманітарної та соціально-економічної підготовки;
- природничо-наукової, професійної та практичної підготовки.

Розподіл змісту програми підготовки фахівця та навчального часу за нормативною та варіативною частинами програми підготовки, навчальний час за циклами підготовки, кількість навчальних годин/кредитів вивчення кожної з навчальних дисциплін і практик нормативної частини програми підготовки подано у таблиці Додатку А.

6 Нормативна частина змісту освітньо-професійної програми

6.1 Система знань у вигляді системи змістових модулів щодо складових узагальнених структур діяльності, поданих у Додатку Б ГСВО ОКХ 8.17010102-12 "Освітньо-кваліфікаційна характеристика", а систему компетенцій, наведено у Додатку Б.

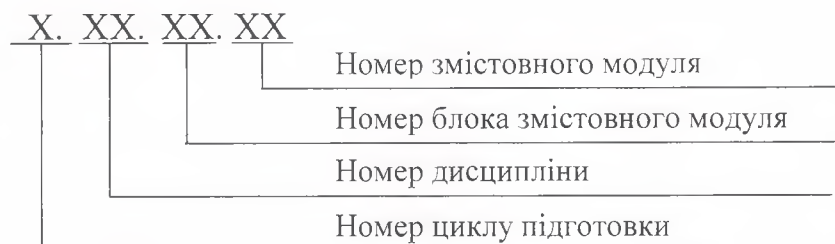
6.2 У таблиці Додатка В подається перелік нормативних навчальних дисциплін й практик (видів практичної підготовки), вказуються назви й шифри блоків змістових модулів, із яких формуються ці навчальні дисципліни й практики, і назви та шифри змістових модулів, що входять до даного блоку змістових модулів.

6.3. У Додатку Г для кожної навчальної дисципліни (або практики) нормативної частини змісту освітньо-професійної програми вказується кількість навчальних годин/національних кредитів/кредитів ECTS її вивчення та перелік сформованих компетенцій.

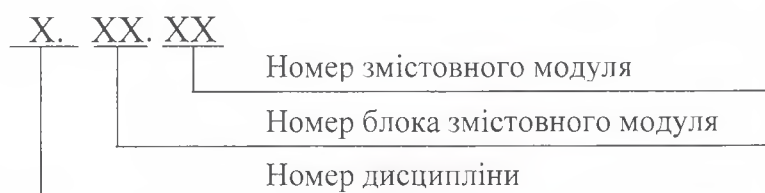
6.4 Нормативна частина ОПП не змінюється.

6.5 Навчальний заклад має право змінювати назви навчальних дисциплін і практик та розподіл блоків змістових модулів у них за окремим погодженням із МОНмолодьспорт України. У додатках Б та В шифри змістовних модулів та змістовних блоків мають наступні структури:

а) шифр блоків змістовних модулів



а) шифр змістовних модулів



7 Державна атестація осіб, які навчаються у вищих навчальних закладах

7.1 На державну атестацію виносяться система компетенцій, що визначена в ГСВОУ ОКХ 8.17010102-12 "Освітньо-кваліфікаційна характеристика" та система блоків відповідних змістових модулів, що зазначена у таблиці Додатка Б.

7.2 Вид кваліфікаційної роботи (дипломний проект або дипломна робота) встановлюється на основі аналізу змісту виробничих функцій та типових задач діяльності, що визначені в ГСВОУ ОКХ 8.17010102-12 "Освітньо-кваліфікаційна характеристика".

7.3 У додатку Д зазначаються нормативні форми державної атестації і подано розподіл блоків змістових модулів між ними.

7.4 Особи, що отримали диплом магістра зі спеціальності 8.17010102 "Безпека державних інформаційних ресурсів" можуть поступати до аспірантури.

8 Вимоги до системи освіти та професійної підготовки

8.1 У викладанні навчальних дисциплін нормативної частини змісту навчання беруть участь доктори наук, професори, кандидати наук, доценти, які мають певний стаж практичної, наукової та педагогічної роботи. Доцільно, щоб викладачі, які забезпечують дисципліни циклу математичної, науково-природничої, професійної та практичної підготовки, у переважній більшості мали наукові ступені в галузі технічних або фізико-математичних наук.

8.2 Викладацький склад, який викладає навчальні дисципліни нормативної частини змісту навчання, повинний мати кваліфікацію, фах за дипломом про вищу освіту та наукову спеціальність за дипломом про отримання наукового ступеня, які відповідають напрямку та спеціальності підготовки магістрів.

8.3 Викладачі, що отримали диплом про вищу освіту за спеціальністю, яка не відповідає напрямку «Безпека інформаційних і комунікаційних систем» та вимогам навчальних дисциплін відповідно до освітньо-професійної програми, повинні мати документи про підвищення кваліфікації у вигляді дипломів кандидатів технічних наук, докторів технічних наук за напрямом спеціальності, що відповідає освітньо-професійній програмі; дипломів, сертифікатів або свідоцтв про післядипломну освіту та підвищення кваліфікації, мати стаж практичної, наукової та педагогічної діяльності, навчальні посібники з відповідного напрямку.

8.4 Науково-педагогічний склад, який здійснює навчальний процес, має періодично та своєчасно проходити стажування. Викладачі, які забезпечують викладання дисциплін циклу професійної та практичної підготовки, мають не рідше ніж раз на п'ять років проходити курси підвищення кваліфікації.

Додаток А

Таблиця 1. Розподілу змісту освітньо-професійної програми та максимальний навчальний час за циклами підготовки

ТЕРМІН НАВЧАННЯ (РОКІВ)	1,5 роки
Максимальний навчальний час загальної підготовки (академічних годин/кредитів/кредитів ECTS)	3240 / 60 / 90
Максимальний навчальний час за циклами (академічних годин/ національних кредитів/кредитів ECTS)	
– гуманітарної та соціально-економічної підготовки	216 / 4 / 6
– природничо-наукової підготовки, професійної та практичної підготовки	1296 / 24 / 36

Таблиця 2. Перелік навчальних дисциплін, форми контролю та державної атестації, нормативний термін навчання

Шифр дис.	Навчальна дисципліна/практика	Академічних годин	Національних кредитів	Кредитів ECTS	Вид контролю
НОРМАТИВНА ЧАСТИНА					
Цикл гуманітарної та соціально-економічної підготовки					
НГ-01	Філософські проблеми наукового пізнання	36	0,67	1	Залік
НГ-02	Педагогіка вищої школи	36	0,67	1	Залік
НГ-03	Основи наукових досліджень	72	1,33	2	Залік
НГ-04	Патентознавство та авторське право	36	0,67	1	Залік
НГ-05	Іноземна мова професійного спрямування	36	0,67	1	Залік
Усього за нормативну частину циклу гуманітарної та соціально-економічної підготовки		216	4	6	10%(1)
Цикл природничо-наукової, професійної та практичної підготовки					
НП-01	Експертиза та сертифікація засобів і систем захисту інформації	54	1,00	1,5	Залік
НП-02	Охорона праці в галузі	72	1,33	2	Іспит
НП-03	Цивільний захист	36	0,67	1	Залік
НП-04	Технології виявлення та блокування загроз до державних інформаційних ресурсів в ІТКС	234	4,33	6,5	Іспит
НП-05	Науково-дослідна практика	72	1,33	2	Залік
НП-06	Переддипломна практика	72	1,33	2	Залік
НП-07	Виконання магістерської роботи	540	10,00	15	Залік
Усього за нормативну частину циклу природничо-наукової, професійної та практичної підготовки		1080	20	30	50%(1)
Усього за нормативну частину		1296	24	36	60%(1)
ВАРІАТИВНА ЧАСТИНА					
	Цикл дисциплін вільного вибору ВНЗ				
	Цикл дисциплін вільного вибору студента				
Усього за варіативну частину		1944	36	54	40%(1,5)
Усього за 1 рік навчання		3240	60	90	100%(1,5)

Додаток Б

Таблиця 3. Система змістовних модулів

Зміст уміння, що забезпечується	Шифр уміння	Назва дисципліни	Назва змістовного модуля	Шифр змістовного модуля
1	2	3	4	5
Аналізувати та систематизувати науково-технічну інформацію вітчизняного та закордонного досвіду з питань захисту інформації	І.ПФ.Д.01.01	Основи наукових досліджень	Організація науково-дослідної роботи студентів та аспірантів	1.03.02.01
			Методологія наукових досліджень	1.03.02.02
			Наукове дослідження і методика його виконання в економіці	1.03.02.03
			Основні напрями наукових досліджень в галузі інформаційної безпеки	1.03.02.04
			Наукова організація дослідного процесу	1.03.02.05
			Інформаційне забезпечення наукових досліджень	1.03.03.01
			Систематизація результатів наукових досліджень	1.03.03.02
			Впровадження результатів наукових досліджень та їх ефективність	1.03.03.03
		Філософські проблеми наукового пізнання	Основні проблеми філософії науки	1.01.01.01
			Основні історичні етапи розвитку науки	1.01.01.02
			Структура наукового пізнання	1.01.01.03
			Динаміка науки, теоретичні моделі та закономірності розвитку	1.01.01.04
			Методологія наукового пізнання	1.01.02.01
			Методи наукового пізнання	1.01.02.02
		Іноземна мова професійного спрямування	Новачі в сучасній науці	1.01.02.03
			Елементи усного та письмового перекладу інформації іноземною мовою в процесі ділових контактів, ділових зустрічей, нарад.	1.02.02.01
			Методика пошуку нової інформації.	1.02.02.02
			Лексичний мінімум інформаційних технологій	1.02.02.03
			Методика реферування професійно-орієнтовані іншомовні джерела.	1.02.03.01
			Особливості комп'ютерного перекладу великих обсягів іншомовної інформації	1.02.03.02
		Технології виявлення та блокування загроз до державних інформаційних ресурсів в ІТКС	Вимоги до захисту інформації в інформаційно-телекомунікаційних систем	2.04.01.01
			Аналіз захищеності сучасних операційних систем	2.04.01.02
			Підходи до проектування систем захисту інформації	2.04.01.03
			Протоколи безпеки, що використовуються в комп'ютерних системах та мережах	2.04.01.04
Технології та методи виявлення загроз програмного забезпечення	2.04.01.08			
Готувати за результатами наукових досліджень звіти, наукові публікації та доповіді на наукових конференціях	І.ПФ.Д.01.02	Філософські проблеми наукового пізнання	Основні проблеми філософії науки	1.01.01.01
			Основні історичні етапи розвитку науки	1.01.01.02
			Структура наукового пізнання	1.01.01.03
			Динаміка науки, теоретичні моделі та закономірності розвитку	1.01.01.04
			Методологія наукового пізнання	1.01.02.01
			Методи наукового пізнання	1.01.02.02
			Новачі в сучасній науці	1.01.02.03
			Предмет і завдання педагогіки вищої школи	1.02.01.01
		Основи наукових досліджень	Основні напрями наукових досліджень в галузі інформаційної безпеки	1.03.02.04
			Наукова організація дослідного процесу	1.03.02.05
			Інформаційне забезпечення наукових досліджень	1.03.03.01
			Систематизація результатів наукових досліджень	1.03.03.02
			Впровадження результатів наукових досліджень та їх ефективність	1.03.03.03
Аналізувати, теоретично та експериментально досліджувати	І.ПФ.Д.01.03	Технології виявлення та	Аналіз захищеності сучасних операційних систем	2.04.01.02

Зміст уміння, що забезпечується	Шифр уміння	Назва дисципліни	Назва змістовного модуля	Шифр змістовного модуля
1	2	3	4	5
методи, алгоритми, програми захисту інформаційних ресурсів		блокування загроз до державних інформаційних ресурсів в ІТКС	Механізми активного та пасивного аналізу інформаційного обміну	2.04.01.07
			Технології та методи виявлення загроз програмного забезпечення	2.04.01.08
Аналізувати, створювати та досліджувати математичні та програмні моделі захисту інформаційних ресурсів	1.ПФ.Д.01.04	Технології виявлення та блокування загроз до державних інформаційних ресурсів в ІТКС	Протоколи безпеки, що використовуються в комп'ютерних системах та мережах	2.04.01.04
			Розповсюдження, обмін, сертифікація та управління ключами в комп'ютерних системах та мережах	2.04.01.05
			Методи забезпечення безпеки бездротових мереж	2.04.01.06
			Механізми активного та пасивного аналізу інформаційного обміну	2.04.01.07
			Технології та методи виявлення загроз програмного забезпечення	2.04.01.08
			Розробка засобів тестування вразливостей	2.04.01.09
			Механізми захисту інформаційних ресурсів інформаційно-телекомунікаційних систем	2.04.02.01
			Механізми, методи та моделі управління доступом до ресурсів інформаційно-телекомунікаційних систем	2.04.02.02
			Застосування апаратного та програмного забезпечення для блокування загроз в інформаційно-телекомунікаційних систем	2.04.02.03
			Визначати та вибирати методи та засоби захисту інформації в автоматизованих системах	1.ПФ.Д.01.05
Механізми, методи та моделі управління доступом до ресурсів інформаційно-телекомунікаційних систем	2.04.02.02			
Застосування апаратного та програмного забезпечення для блокування загроз в інформаційно-телекомунікаційних систем	2.04.02.03			
Проводити аналіз вразливостей та ефективності засобів, методів захисту автоматизованих систем	1.ПФ.Д.01.06	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Механізми активного та пасивного аналізу інформаційного обміну	2.04.01.07
			Технології та методи виявлення загроз програмного забезпечення	2.04.01.08
			Розробка засобів тестування вразливостей	2.04.01.09
			Аналіз захищеності сучасних операційних систем	2.04.01.02
Виконувати експериментально-дослідні роботи щодо атестації автоматизованих систем	1.ПФ.Д.01.07	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Вимоги до захисту інформації в інформаційно-телекомунікаційних систем	2.04.01.01
			Аналіз захищеності сучасних операційних систем	2.04.01.02
			Підходи до проектування систем захисту інформації	2.04.01.03
Виконувати експериментально-дослідні роботи при проведенні сертифікації засобів захисту інформації та аналізувати отримані результати	1.ПФ.Д.01.08	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Підходи до проектування систем захисту інформації	2.04.01.03
			Протоколи безпеки, що використовуються в комп'ютерних системах та мережах	2.04.01.04
			Розповсюдження, обмін, сертифікація та управління ключами в комп'ютерних системах та мережах	2.04.01.05
			Методи забезпечення безпеки бездротових мереж	2.04.01.06
			Механізми активного та пасивного аналізу інформаційного обміну	2.04.01.07
			Технології та методи виявлення загроз програмного забезпечення	2.04.01.08
Організовувати роботи щодо виконання вимог режиму захисту інформації та забезпеченню захисту державної таємниці	2.ПФ.С.01.01	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Розробка засобів тестування вразливостей	2.04.01.09
			Аналіз захищеності сучасних операційних систем	2.04.01.02
			Підходи до проектування систем захисту інформації	2.04.01.03
Організовувати роботи щодо тестування та налагодження програмно-апаратних криптографічних та технічних систем і	2.ПФ.С.01.02	Технології виявлення та блокування загроз державним	Розповсюдження, обмін, сертифікація та управління ключами в комп'ютерних системах та мережах	2.04.01.05
			Механізми захисту інформаційних ресурсів інформаційно-телекомунікаційних систем	2.04.02.01

Зміст уміння, що забезпечується	Шифр уміння	Назва дисципліни	Назва змістовного модуля	Шифр змістовного модуля
1	2	3	4	5
засобів забезпечення захисту інформації		інформаційним ресурсам в ІТКС	Механізми, методи та моделі управління доступом до ресурсів інформаційно-телекомунікаційних систем	2.04.02.02
			Застосування апаратного та програмного забезпечення для блокування загроз в інформаційно-телекомунікаційних систем	2.04.02.03
Розробляти пропозиції щодо підвищення ефективності прийнятих заходів по забезпеченню захисту інформації в інформаційно-телекомунікаційних системах	2.ПФ.С.01.03	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Механізми захисту інформаційних ресурсів інформаційно-телекомунікаційних систем	2.04.02.01
			Механізми, методи та моделі управління доступом до ресурсів інформаційно-телекомунікаційних систем	2.04.02.02
			Застосування апаратного та програмного забезпечення для блокування загроз в інформаційно-телекомунікаційних систем	2.04.02.03
Проводити перевірки працездатності та ефективності програмно-апаратних засобів захисту інформації, що застосовуються	2.ПФ.С.01.04	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Механізми активного та пасивного аналізу інформаційного обміну	2.04.01.07
			Технології та методи виявлення загроз програмного забезпечення	2.04.01.08
			Механізми захисту інформаційних ресурсів інформаційно-телекомунікаційних систем	2.04.02.01
			Механізми, методи та моделі управління доступом до ресурсів інформаційно-телекомунікаційних систем	2.04.02.02
			Застосування апаратного та програмного забезпечення для блокування загроз в інформаційно-телекомунікаційних систем	2.04.02.03
Організовувати роботу щодо розробки проектів документів сертифікації засобів та систем захисту інформації	2.ПФ.С.02.01	Експертиза та сертифікація засобів і систем захисту інформації	Сертифікації засобів захисту інформації	2.01.01.01
			Експертизи засобів захисту інформації	2.01.01.02
Організовувати роботу щодо допуску до експлуатації засобів захисту інформації систем спеціального зв'язку	2.ПФ.С.02.02	Експертиза та сертифікація засобів і систем захисту інформації	Тематичні дослідження засобів захисту інформації систем спеціального зв'язку	2.01.02.01
Організовувати роботу щодо розробки проектів документів експертизи засобів та систем захисту інформації	2.ПФ.С.02.03	Експертиза та сертифікація засобів і систем захисту інформації	Сертифікації систем захисту інформації	2.01.03.01
			Експертизи систем захисту інформації	2.01.03.02
Організовувати виробничу діяльність у відповідності з вимогами законодавчих та нормативно-правових документів з питань охорони праці	2.СВ.С.01.01	Охорона праці в галузі	Правове забезпечення та основні положення організації охорони праці в Україні та Держспецзв'язку	2.02.01.01
Оцінювати стан виконання вимог керівних документів з питань охорони праці на об'єктах (підрозділах) органів державної влади	2.СВ.С.01.02	Охорона праці в галузі	Правове забезпечення та основні положення організації охорони праці в Україні	2.02.01.01
			Організація пожежної безпеки підрозділу (об'єкту) органів державної влади	2.02.02.01
Визначити та аналізувати параметри умов праці особового складу, розробляти заходи щодо нормалізації факторів виробничого середовища та пожежної безпеки об'єкту (підрозділу) органів державної влади	2.СВ.С.01.03	Охорона праці в галузі	Організація навчання та допуску особового складу до самостійного виконання посадових обов'язків	2.02.01.02
			Параметри умов праці особового складу підрозділу (об'єкту) спеціального зв'язку, заходи та засоби їх оптимізації	2.02.02.02
Проводити наради, інструктажі та заняття з особовим складом з питань охорони праці та техніки безпеки, відпрацьовувати необхідну документацію підрозділу з охорони праці	2.СВ.С.01.04	Охорона праці в галузі	Організація та забезпечення безпеки особового складу при експлуатації засобів спеціального зв'язку	2.02.02.03
Організовувати заходи щодо забезпечення охорони праці в підрозділах інформаційної безпеки	2.СВ.С.01.05	Цивільний захист	Цивільний захист України в сучасних умовах. Роль і місце цивільного захисту в державній системі безпеки людини	2.03.01.01
			Надзвичайні ситуації воєнного характеру та загальна характеристика їх можливих наслідків	2.03.01.02

Зміст уміння, що забезпечується	Шифр уміння	Назва дисципліни	Назва змістовного модуля	Шифр змістовного модуля
1	2	3	4	5
			Надзвичайні ситуації мирного часу та їх вплив на життєдіяльність людей. Загальна характеристика можливих надзвичайних ситуацій в Україні	2.03.01.03
			Основні принципи і способи захисту населення при аваріях, катастрофах, стихійних лихах та застосуванні зброї, їх стисла характеристика	2.03.01.04
			Дії населення за сигналами оповіщення цивільного захисту. Евакуація та порядок її проведення	2.03.02.01
Організовувати заходи цивільного захисту в умовах надзвичайних ситуацій мирного часу	2.СВ.С.02.01	Цивільний захист	Цивільний захист України в сучасних умовах. Роль і місце цивільного захисту в державній системі безпеки людини	2.03.01.01
			Надзвичайні ситуації воєнного характеру та загальна характеристика їх можливих наслідків	2.03.01.02
			Надзвичайні ситуації мирного часу та їх вплив на життєдіяльність людей. Загальна характеристика можливих надзвичайних ситуацій в Україні	2.03.01.03
			Основні принципи і способи захисту населення при аваріях, катастрофах, стихійних лихах та застосуванні зброї, їх стисла характеристика	2.03.01.04
			Дії населення за сигналами оповіщення цивільного захисту. Евакуація та порядок її проведення	2.03.02.01
			Організація навчання керівників, посадових осіб і населення з питань цивільного захисту та їх підготовка до дій в надзвичайних ситуаціях	2.03.02.02
			Мета, зміст і умови проведення аварійно-рятувальних та інших невідкладних робіт в осередках надзвичайних ситуацій	2.03.02.03
			Організація і планування заходів цивільного захисту на об'єкті господарської діяльності. Структура системи цивільного захисту об'єкта	2.03.02.04
Застосовувати вбудовані механізми захисту сучасних операційних систем	3.ПФ.Е.01.01	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Механізми захисту інформаційних ресурсів інформаційно-телекомунікаційних систем	2.04.02.01
			Механізми, методи та моделі управління доступом до ресурсів інформаційно-телекомунікаційних систем	2.04.02.02
			Застосування апаратного та програмного забезпечення для блокування загроз в інформаційно-телекомунікаційних систем	2.04.02.03
Розробляти та аналізувати засоби тестування вразливостей	3.ПФ.Е.01.02	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Механізми активного та пасивного аналізу інформаційного обміну	2.04.01.07
			Технології та методи виявлення загроз програмного забезпечення	2.04.01.08
			Розробка засобів тестування вразливостей	2.04.01.09
Розробляти вимоги та специфікації обладнання, засобів та методів, що застосовуються для захисту інформаційно-телекомунікаційних систем	3.ПФ.Е.01.03	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Механізми активного та пасивного аналізу інформаційного обміну	2.04.01.07
			Технології та методи виявлення загроз програмного забезпечення	2.04.01.08
			Розробка засобів тестування вразливостей	2.04.01.09
			Механізми захисту інформаційних ресурсів інформаційно-телекомунікаційних систем	2.04.02.01
			Механізми, методи та моделі управління доступом до ресурсів інформаційно-телекомунікаційних систем	2.04.02.02
			Застосування апаратного та програмного забезпечення для блокування загроз в інформаційно-телекомунікаційних систем	2.04.02.03
Застосовувати засоби пасивного збору інформації та контролю працездатності серверів	3.ПФ.Е.01.04	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Механізми активного та пасивного аналізу інформаційного обміну	2.04.01.07
			Технології та методи виявлення загроз програмного забезпечення	2.04.01.08
			Розробка засобів тестування вразливостей	2.04.01.09

Зміст уміння, що забезпечується	Шифр уміння	Назва дисципліни	Назва змістовного модуля	Шифр змістовного модуля
1	2	3	4	5
Застосовувати мережеві екрани та маскуванню структури мережевих ресурсів	3.ПФ.Е.01.05	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Механізми захисту інформаційних ресурсів інформаційно-телекомунікаційних систем	2.04.02.01
			Механізми, методи та моделі управління доступом до ресурсів інформаційно-телекомунікаційних систем	2.04.02.02
			Застосування апаратного та програмного забезпечення для блокування загроз в інформаційно-телекомунікаційних систем	2.04.02.03
Застосовувати механізми розподілу доступу до інформаційних ресурсів систем управління базами даних	3.ПФ.Е.01.06	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Механізми захисту інформаційних ресурсів інформаційно-телекомунікаційних систем	2.04.02.01
			Механізми, методи та моделі управління доступом до ресурсів інформаційно-телекомунікаційних систем	2.04.02.02
			Застосування апаратного та програмного забезпечення для блокування загроз в інформаційно-телекомунікаційних систем	2.04.02.03
Застосовувати віртуальні мережі, списки доступу та системи відновлення працездатності засобів маршрутизації	3.ПФ.Е.01.07	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Механізми захисту інформаційних ресурсів інформаційно-телекомунікаційних систем	2.04.02.01
			Механізми, методи та моделі управління доступом до ресурсів інформаційно-телекомунікаційних систем	2.04.02.02
			Застосування апаратного та програмного забезпечення для блокування загроз в інформаційно-телекомунікаційних систем	2.04.02.03
Оцінювати, вибирати та розробляти необхідні методики пошуку вразливостей захисту автоматизованих систем	3.ПФ.Е.01.08	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Механізми активного та пасивного аналізу інформаційного обміну	2.04.01.07
			Технології та методи виявлення загроз програмного забезпечення	2.04.01.08
			Аналіз захищеності сучасних операційних систем	2.04.01.02
			Розробка засобів тестування вразливостей	2.04.01.09
Проводити моніторинг інформаційної безпеки автоматизованих систем	4.ПФ.Е.01.09	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Аналіз захищеності сучасних операційних систем	2.04.01.02
			Механізми активного та пасивного аналізу інформаційного обміну	2.04.01.07
			Технології та методи виявлення загроз програмного забезпечення	2.04.01.08
			Розробка засобів тестування вразливостей	2.04.01.09
Забезпечувати захист програмного та інформаційного забезпечення від несанкціонованих дій	4.ПФ.Е.01.01	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Механізми захисту інформаційних ресурсів інформаційно-телекомунікаційних систем	2.04.02.01
			Механізми, методи та моделі управління доступом до ресурсів інформаційно-телекомунікаційних систем	2.04.02.02
			Застосування апаратного та програмного забезпечення для блокування загроз в інформаційно-телекомунікаційних систем	2.04.02.03
Застосовувати вбудовані механізми захисту сучасних операційних систем	4.ПФ.Е.01.02	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Механізми захисту інформаційних ресурсів інформаційно-телекомунікаційних систем	2.04.02.01
			Механізми, методи та моделі управління доступом до ресурсів інформаційно-телекомунікаційних систем	2.04.02.02
			Застосування апаратного та програмного забезпечення для блокування загроз в інформаційно-телекомунікаційних систем	2.04.02.03
Застосовувати розроблені механізми та методи захисту інформаційних ресурсів	4.ПФ.Е.01.03	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Механізми захисту інформаційних ресурсів інформаційно-телекомунікаційних систем	2.04.02.01
			Механізми, методи та моделі управління доступом до ресурсів інформаційно-телекомунікаційних систем	2.04.02.02
			Застосування апаратного та програмного забезпечення для блокування загроз в інформаційно-телекомунікаційних систем	2.04.02.03
Реалізовувати та тестувати компоненти програмного	4.ПФ.Е.01.04	Технології виявлення та	Технології та методи виявлення загроз програмного забезпечення	2.04.01.08

Зміст уміння, що забезпечується	Шифр уміння	Назва дисципліни	Назва змістовного модуля	Шифр змістовного модуля
1	2	3	4	5
забезпечення із захисту інформації		блокування загроз державним інформаційним ресурсам в ІТКС	Розробка засобів тестування вразливостей Механізми захисту інформаційних ресурсів інформаційно-телекомунікаційних систем	2.04.01.09 2.04.02.01
Застосовувати протоколи захисту інформації, мережевих сервісів та сервісів додатків	4.ПФ.Е.01.05	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Протоколи безпеки, що використовуються в комп'ютерних системах та мережах Механізми захисту інформаційних ресурсів інформаційно-телекомунікаційних систем Механізми, методи та моделі управління доступом до ресурсів інформаційно-телекомунікаційних систем	2.04.01.04 2.04.02.01 2.04.02.02
Встановлювати, робити монтаж, налаштувати, експлуатувати та обслуговувати програмно-апаратні засоби захисту інформації	4.ПФ.Е.01.06	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Механізми, методи та моделі управління доступом до ресурсів інформаційно-телекомунікаційних систем Застосування апаратного та програмного забезпечення для блокування загроз в інформаційно-телекомунікаційних систем	2.04.02.02 2.04.02.03
Адмініструвати підсистеми інформаційної безпеки автоматизованої системи	4.ПФ.Е.01.07	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Розповсюдження, обмін, сертифікація та управління ключами в комп'ютерних системах та мережах Методи забезпечення безпеки бездротових мереж Механізми активного та пасивного аналізу інформаційного обміну Технології та методи виявлення загроз програмного забезпечення Розробка засобів тестування вразливостей Механізми захисту інформаційних ресурсів інформаційно-телекомунікаційних систем Механізми, методи та моделі управління доступом до ресурсів інформаційно-телекомунікаційних систем Застосування апаратного та програмного забезпечення для блокування загроз в інформаційно-телекомунікаційних систем	2.04.01.05 2.04.01.06 2.04.01.07 2.04.01.08 2.04.01.09 2.04.02.01 2.04.02.02 2.04.02.03
Управляти інформаційною безпекою автоматизованої системи	4.ПФ.Е.01.08	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Розповсюдження, обмін, сертифікація та управління ключами в комп'ютерних системах та мережах Методи забезпечення безпеки бездротових мереж Механізми активного та пасивного аналізу інформаційного обміну Технології та методи виявлення загроз програмного забезпечення Розробка засобів тестування вразливостей Механізми захисту інформаційних ресурсів інформаційно-телекомунікаційних систем Механізми, методи та моделі управління доступом до ресурсів інформаційно-телекомунікаційних систем Застосування апаратного та програмного забезпечення для блокування загроз в інформаційно-телекомунікаційних систем	2.04.01.05 2.04.01.06 2.04.01.07 2.04.01.08 2.04.01.09 2.04.02.01 2.04.02.02 2.04.02.03

Додаток В

Таблиця 4. Рекомендований перелік навчальних дисциплін

Шифр навч дисц	Назва навчальної дисципліни	Назви блоків змістовних модулів, що входять до навчальної дисципліни	Шифри блоків змістовних модулів	Назви змістовних модулів навчальної дисципліни	Шифри змістовних модулів
1	2	3	4	5	6
1. Цикл дисциплін гуманітарної та соціально-економічної підготовки					
1.01	Філософські проблеми наукового пізнання	Наукове знання та його особливості	1.01.01	Основні проблеми філософії науки	1.01.01.01
				Основні історичні етапи розвитку науки	1.01.01.02
				Структура наукового пізнання	1.01.01.03
				Динаміка науки, теоретичні моделі та закономірності розвитку	1.01.01.04
	Основи методології наукового пізнання	1.01.02	Методологія наукового пізнання	1.01.02.01	
			Методи наукового пізнання	1.01.02.02	
			Новачі в сучасній науці	1.01.02.03	
1.02	Педагогіка вищої школи	Загальні основи педагогіки вищої школи	1.02.01	Предмет і завдання педагогіки вищої школи	1.02.01.01
				Педагогічний процес у вищій школі	1.02.01.02
				Теорія і практика освіти	1.02.01.03
				Болонський процес і освіта в Україні	1.02.01.04
		Дидактика вищої школи	1.02.02	Дидактичні системи та дидактичні технології у вищій школі	1.02.02.01
				Види і стилі навчання	1.02.02.02
				Зміст освіти у вищих навчальних закладах	1.02.02.03
				Закони, принципи та закономірності навчання	1.02.02.04
		Методи та форми організації навчання у вищій школі	1.02.03	Поняття методів навчання, їх класифікація	1.02.03.01
				Загальна характеристика форм організації навчання у вищій школі	1.02.03.02
				Методика організації та проведення лекційних, практичних, лабораторних і семінарських занять у вищій школі	1.02.03.03
				Методика організації та проведення індивідуальних занять, консультації, колоквиуму, ігор	1.02.03.04
				Самостійна робота студентів та її методика	1.02.03.05
				Поняття контролю навчальної діяльності студентів: функції, принципи організації, види та форми	1.02.03.06
				Оцінка й оцінювання у вищій школі, засоби діагностики	1.02.03.07
				Виховання у вищому навчальному закладі	1.02.04
Закони, закономірності та основні принципи виховання студентів	1.02.04.02				
Методи, форми і засоби виховного впливу на особистість студента	1.02.04.03				
Самовиховання студентів в умовах вищих навчальних закладів та його мотивація	1.02.04.04				
Науково-педагогічний працівник вищого навчального закладу	1.02.05	Роль і місце науково-педагогічного працівника в розвитку суспільства, його функції	1.02.05.01		
		Особливості педагогічної діяльності у ВНЗ	1.02.05.02		
1.03	Основи наукових досліджень	Основи наукознавства	1.03.01	Роль та завдання науки при переході до ринкової економіки	1.03.01.01
				Основні напрямки наукових економічних досліджень в сучасних умовах	1.03.01.02
		Основи методології науково-дослідної роботи	1.03.02	Організація науково-дослідної роботи студентів та аспірантів	1.03.02.01
				Методологія наукових досліджень	1.03.02.02
		Наукове дослідження і методика його виконання	1.03.02.03		

Шифр навч дисц	Назва навчальної дисципліни	Назви блоків змістовних модулів, що входять до навчальної дисципліни	Шифри блоків змістовних модулів	Назви змістовних модулів навчальної дисципліни	Шифри змістовних модулів
1	2	3	4	5	6
				Основні напрями наукових досліджень в галузі інформаційної безпеки	1.03.02.04
				Наукова організація дослідного процесу	1.03.02.05
		Оформлення та форми впровадження результатів наукового дослідження	1.03.03	Інформаційне забезпечення наукових досліджень	1.03.03.01
				Систематизація результатів наукових досліджень	1.03.03.02
				Впровадження результатів наукових досліджень та їх ефективність	1.03.03.03
1.04	Патентознавство та авторське право	Система охорони інтелектуальної власності	1.04.01	Система інтелектуальної власності в Україні	1.04.01.01
				Міжнародне співробітництво у сфері інтелектуальної власності	1.04.01.02
		Створення і патентно-інформаційні дослідження об'єктів промислової власності	1.04.02	Методологічні основи створення об'єктів промислової власності	1.04.02.01
				Патентна інформація та документація	1.04.02.02
				Патентні дослідження	1.04.02.03
		Охорона і захист об'єктів промислової власності	1.04.03	Охорона прав на винаходи і корисні моделі	1.04.03.01
				Оформлення заявки на винахід (корисну модель)	1.04.03.02
				Охорона прав на промислові зразки	1.04.03.03
				Охорона прав на фірмові найменування та знаки для товарів і послуг	1.04.03.04
				Охорона прав на топографії інтегральних мікросхем	1.04.03.05
				Охорона прав на раціоналізаторські пропозиції і науково-технічну інформацію	1.04.03.06
		Охорона і захист авторського права та суміжних прав	1.04.04	Авторське право	1.04.04.01
				Суміжні права	1.04.04.02
		Організація і економіка інтелектуальної власності	1.04.05	Ліцензування і передача технологій	1.04.05.01
				Економічна ефективність використання об'єктів інтелектуальної власності	1.04.05.02
1.05	Іноземна мова професійного спрямування	Аудіювання, мовлення, читання	1.05.01	Елементи усного та письмового перекладу інформації іноземною мовою в процесі ділових контактів, ділових зустрічей, нарад.	1.05.01.01
				Лексико-граматичний мінімум забезпечення та мовно-комунікативний рівень проведення переговорів	1.05.01.02
		Елементи усного та письмового перекладу інформації іноземною мовою	1.05.02	Елементи усного та письмового перекладу інформації іноземною мовою в процесі ділових контактів, ділових зустрічей, нарад.	1.05.02.01
				Методика пошуку нової інформації	1.05.02.02
				Лексичний мінімум інформаційних технологій	1.05.02.03
		Професійно-орієнтовані іншомовні джерела	1.05.03	Методика реферування професійно-орієнтованих іншомовних джерел.	1.05.03.01
				Особливості комп'ютерного перекладу великих обсягів іншомовної інформації	1.05.03.02
2. Цикл природничо-наукової, професійної та практичної підготовки					
2.01	Експертиза та сертифікація засобів і систем захисту інформації	Основи експертизи та сертифікації засобів захисту інформації	2.01.01	Сертифікації засобів захисту інформації	2.01.01.01
				Експертизи засобів захисту інформації	2.01.01.02
		Основи експертизи та сертифікації систем захисту інформації	2.01.02	Сертифікації систем захисту інформації	2.01.02.01
				Експертизи систем захисту інформації	2.01.02.02
		Допуск до експлуатації засобів захисту інформації систем спеціального зв'язку	2.01.03	Тематичні дослідження засобів захисту інформації систем спеціального зв'язку	2.01.03.01
2.02	Охорона праці в галузі	Організація охорони праці в галузі інформаційної безпеки	2.02.01	Правове забезпечення та основні положення організації охорони праці в Україні в галузі інформаційної безпеки	2.02.01.01
				Організація навчання та допуску особового складу до самостійного виконання посадових обов'язків	2.02.01.02
		Організація та забезпечення безпеки	2.02.02	Організація пожежної безпеки підрозділу (об'єкту) Держспецзв'язку	2.02.02.01

Шифр навч дисц	Назва навчальної дисципліни	Назви блоків змістовних модулів, що входять до навчальної дисципліни	Шифри блоків змістовних модулів	Назви змістовних модулів навчальної дисципліни	Шифри змістовних модулів
1	2	3	4	5	6
		особового складу при експлуатації засобів спеціального зв'язку		Параметри умов праці особового складу підрозділу (об'єкту) спеціального зв'язку, заходи та засоби їх оптимізації	2.02.02.02
				Організація та забезпечення безпеки особового складу при експлуатації засобів спеціального зв'язку	2.02.02.03
2.03	Цивільний захист	Моніторинг та визначення рівня небезпеки надзвичайних ситуацій	2.03.01	Цивільний захист України в сучасних умовах. Роль і місце цивільного захисту в державній системі безпеки людини	2.03.01.01
				Надзвичайні ситуації воєнного характеру та загальна характеристика їх можливих наслідків	2.03.01.02
				Надзвичайні ситуації мирного часу та їх вплив на життєдіяльність людей. Загальна характеристика можливих надзвичайних ситуацій в Україні	2.03.01.03
				Основні принципи і способи захисту населення при аваріях, катастрофах, стихійних лихах та застосуванні зброї, їх стисла характеристика	2.03.01.04
		Планування, організація та проведення заходів цивільного захисту	2.03.02	Дії населення за сигналами оповіщення цивільного захисту. Евакуація та порядок її проведення	2.03.02.01
				Організація навчання керівників, посадових осіб і населення з питань цивільного захисту та їх підготовка до дій в надзвичайних ситуаціях	2.03.02.02
				Мета, зміст і умови проведення аварійно-рятувальних та інших невідкладних робіт в осередках надзвичайних ситуацій	2.03.02.03
				Організація і планування заходів цивільного захисту на об'єкті господарської діяльності. Структура системи цивільного захисту об'єкта	2.03.02.04
2.04	Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	Технології виявлення загроз інформаційних ресурсів в ІТКС	2.04.01	Вимоги до захисту інформації в інформаційно-телекомунікаційних систем	2.04.01.01
				Аналіз захищеності сучасних операційних систем	2.04.01.02
				Підходи до проектування систем захисту інформації	2.04.01.03
				Протоколи безпеки, що використовуються в комп'ютерних системах та мережах	2.04.01.04
				Розповсюдження, обмін, сертифікація та управління ключами в комп'ютерних системах та мережах	2.04.01.05
				Методи забезпечення безпеки бездротових мереж	2.04.01.06
				Механізми активного та пасивного аналізу інформаційного обміну	2.04.01.07
				Технології та методи виявлення загроз програмного забезпечення	2.04.01.08
				Розробка засобів тестування вразливостей	2.04.01.09
				Форензика	2.04.01.10
		Технології блокування загроз в ІТКС	2.04.02	Механізми захисту інформаційних ресурсів інформаційно-телекомунікаційних систем	2.04.02.01
				Механізми, методи та моделі управління доступом до ресурсів інформаційно-телекомунікаційних систем	2.04.02.02
				Застосування апаратного та програмного забезпечення для блокування загроз в інформаційно-телекомунікаційних систем	2.04.02.03

Додаток Г

Таблиця 5. Розподіл змісту освітньо-професійної програми підготовки, навчальний час за циклами підготовки магістра за спеціальністю 8.170102 "Безпека державних інформаційних ресурсів", навчальними дисциплінами й практиками та перелік сформованих компетенцій

Цикл	Навчальні цикли	Перелік дисциплін	Загальна кількість годин	Кредитів нац.	Кредитів ECTS	Шифри сформованих компетенцій
1	2	3	4	5	6	7
ГСЕ (норматив на частину)	Цикл гуманітарної та соціально-економічної підготовки	Філософські проблеми наукового пізнання	36	0,67	1	КСО.01, КСО.02, КСО.03, КСО.04, КСО.05, КСО.06, КСО.07, КСО.08, КСО.09, КСО.10, КСО.11, КСО.12, КСО.13, КІ.01, КІ.02, КІ.03, КІ.05
		Педагогіка вищої школи	36	0,67	1	КСО.01, КСО.02, КСО.04, КСО.05, КСО.06, КСО.07, КСО.08, КСО.09, КСО.11, КСО.12, КСО.13, КІ.01, КІ.02, КІ.03, КІ.04, КІ.05, КЗП.05, КЗП.06
		Основи наукових досліджень	72	1,33	2	КІ.01, КІ.03, КЗН.01, КЗН.02, КЗП.01, КЗП.05, КЗП.06,
		Патентознавство та авторське право	36	0,67	1	КСО.16, КІ.01, КІ.03, КЗН.01, КЗН.02, КЗП.01
		Іноземна мова професійного спрямування	36	0,67	1	КІ.01, КІ.06, КЗП.01
		Всього за цикл:	216	4	6	
ПНППП (норматив на частину)	Цикл природничо-наукової, професійної та практичної підготовки	Експертиза та сертифікація засобів і систем захисту інформації	54	1,00	1,5	КЗП.01, КЗП.02, КЗП.03, КЗП.04, КЗП.05, КЗП.07, КЗП.08, КСП.01, КСП.05, КСП.06
		Охорона праці в галузі	72	1,33	2	КСО.15, КСО.02, КЗП.01
		Цивільний захист	36	0,67	1	КСО.14, КСО.02, КЗП.01
		Технології виявлення та блокування загроз державним інформаційним ресурсам в ІТКС	234	4,33	6,5	КІ.01, КІ.02, КІ.03, КІ.04, КІ.05, КІ.06, КЗН.01, КЗН.02, КЗП.01, КЗП.02, КЗП.03, КЗП.04, КЗП.05, КЗП.05, КСП.01, КСП.02, КСП.03, КСП.04, КСП.07, КСП.08, КСП.09
		Науково-дослідна практика	72	1,33	2	КСО.17, КСО.18, КІ.05, КІ.06, КЗП.01, КСП.01
		Переддипломна практика	72	1,33	2	КСО.17, КСО.18, КІ.05, КІ.06, КЗП.01, КСП.01
		Виконання магістерської роботи	540	10,00	15	КСО.17, КСО.18, КІ.01, КІ.02, КІ.03, КІ.04, КІ.05, КІ.06, КЗН.01, КЗН.02, КЗП.01, КЗП.02, КЗП.03, КЗП.04, КЗП.05, КЗП.05, КСП.01, КСП.02, КСП.03, КСП.04, КСП.07, КСП.08, КСП.09, КСП.10., КСП.11, КСП.12
		Всього за цикл:	1080	20	30	
		Нормативна частина:	1296	24	36	
		Варіативна частина:	1944	36	54	
Всього:	3240	60	90			

Додаток Д
Нормативні форми державної атестації осіб,
які навчаються за спеціальністю 8.170102 "Безпека державних інформаційних ресурсів"

Нормативні форми державної атестації, що використовуються для встановлення рівня опанування особами, які навчаються у вищих навчальних закладах, відповідних змістових модулів:

Дипломний проект (робота) – 1.03.01.01, 1.03.01.02, 1.03.02.01, 1.03.02.02, 1.03.02.03, 1.03.02.04, 1.03.02.05, 1.03.03.01, 1.03.03.02, 1.03.03.03, 2.01.01.01, 2.01.01.02, 2.01.02.01, 2.01.02.02, 2.01.03.01, 2.04.01.01, 2.04.01.02, 2.04.01.03, 2.04.01.04, 2.04.01.05, 2.04.01.06, 2.04.01.07, 2.04.01.08, 2.04.01.09, 2.04.01.10, 2.04.02.01, 2.04.02.02, 2.04.02.03

(шифри змістових модулів, що виносяться на державну атестацію)