

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

ЗАТВЕРДЖЕНО

Рішення Науково-методичної ради Національної академії СБ України від 21 липня 2016 року, протокол № 12

Перший проректор (з навчальної роботи)
Національної академії СБ України
27 липня 2016 року

(у редакції рішення Вченої ради Національної академії СБ України від 28.03.2019 р., протокол №5)

Перший проректор (з навчальної роботи)
Національної академії СБ України
28 березня 2019 року

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

**«МЕНЕДЖМЕНТ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ»
ДРУГОГО (МАГІСТЕРСЬКОГО) РІВНЯ ВИЩОЇ ОСВІТИ**

за спеціальністю 073 «Менеджмент»

галузі знань 07 «Управління та адміністрування»

кваліфікація магістр менеджменту, професіонал із організації захисту
інформації з обмеженим доступом

Розробники освітньо-професійної програми другого (магістерського) рівня вищої освіти:

завідувач СК-32 ННІ ІБ НА СБ України, доктор історичних наук, професор, **Гуз Анатолій Михайлович;**

заступник завідувача СК-32 ННІ ІБ НА СБ України кандидат юридичних наук, доцент **Ткачук Тарас Юрійович;**

професор СК-32 ННІ ІБ НА СБ України кандидат юридичних наук, старший науковий співробітник **Князєв Сергій Олександрович;**

доцент СК-32 ННІ ІБ НА СБ України кандидат юридичних наук, доцент **Касперський Ігор Петрович;**

начальник департаменту охорони державної таємниці Служби безпеки України **Болдир Сергій Володимирович;**

студент Навчально-наукового інститут інформаційної безпеки **Пастушенко Валентин Романович**

Освітньо-професійну програму другого (магістерського) рівня вищої освіти схвалено на засіданні Вченої ради Навчально-наукового інституту інформаційної безпеки НА СБ України від 02 липня 2016 року, протокол № 12.

Голова Вченої ради Навчально-наукового інституту інформаційної безпеки НА СБ України, 2 липня 2016 року

Реєстр. № _____
від _____ 20__ р.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА

Профіль програми	
<p>Рівень вищої освіти – освітньо-професійна програма другого (магістерського) рівня вищої освіти;</p> <p>Ступінь, що присвоюється – магістр;</p> <p>Назва галузі знань – 07 Управління та адміністрування;</p> <p>Назва спеціальності – 073 Менеджмент (спеціалізація – організація захисту інформації з обмеженим доступом);</p> <p>Обмеження щодо форми навчання – відсутні;</p> <p>Освітня кваліфікація, що присвоюється – магістр менеджменту;</p> <p>Кваліфікація в дипломі – магістр менеджменту, професіонал із організації захисту інформації з обмеженим доступом;</p> <p>2149.2 Професіонал із організації захисту інформації з обмеженим доступом: відповідно до Національного класифікатора України: «Класифікатор професій» ДК 003:2010, «Довідника типових професійно-кваліфікаційних характеристик основних посад керівників та інших працівників РСО державної влади, органів місцевого самоврядування, підприємств, установ, організацій», наказ СБ України від 14.07.2003 №293/ДСК, зареєстрований Міністерством юстиції України 05.08. 2003 р. за №685/8006, Довідника кваліфікаційних характеристик професій працівників «Безпека господарської діяльності підприємств установ організацій». – К., 2011.</p>	
<i>Вищий навчальний заклад</i>	Національна академія СБ України, Київ
<i>Акредитаційна інституція</i>	Національна агенція забезпечення якості вищої освіти
<i>Період акредитації</i>	Програма впроваджується в 2016 році
<i>Рівень програми</i>	FQ-EHEA – другий цикл, QF-LLL – 7 рівень, НРК – 8 рівень.
А	Ціль програми
	Формування та розвиток спеціально-професійних компетентностей у галузі менеджменту захисту інформації з обмеженим доступом та провадження діяльності пов'язаної з охороною державної таємниці установ, підприємств, організацій. Забезпечити здобувачам вищої освіти здобуття поглиблених теоретичних й практичних знань, умінь навичок за відповідною спеціалізацією, загальних засад методології професійної діяльності для виконання завдань інноваційної діяльності.
В	Характеристика програми
<i>Опис предметної області</i>	<p>Об'єктами вивчення: управління організаціями та їх підрозділами.</p> <p>Цілі навчання: підготовка фахівців, здатних ідентифікувати та розв'язувати складні задачі і проблеми у сфері менеджменту або у процесі навчання, що передбачають проведення досліджень та або здійснення інновацій та характеризуються невизначеністю умов і вимог.</p> <p>Теоретичний зміст предметної області:</p> <ul style="list-style-type: none"> - парадигми, закони, закономірності; - принципи, історичні передумови розвитку менеджменту - концепції системного, ситуативного, адаптивного, антисипативного, антикризового, інноваційного, проектного менеджменту тощо; - функції методи, технології та управлінські рішення у менеджменті. <p>Методи, методики та технології:</p> <ul style="list-style-type: none"> - загальнонаукові та специфічні методи дослідження; - методи реалізації функцій менеджменту; - методи менеджменту; - теоретичні обґрунтування управлінських рішень. <p>Інструментарій та обладнання: сучасне інформаційно-комунікаційне обладнання, інформаційні системи та програмні продукти, що застосовуються у менеджменті.</p>
<i>Фокус програми: загальна/</i>	Загальні аспекти освітньої програми: «Менеджмент захисту інформації з обмеженим доступом» ґрунтуються на адаптації та

	<i>спеціальна</i>	<p>впровадженні в професійну діяльність знань та навичок для вирішення завдань в менеджменті організацій, кризовому менеджменті та ведення кадрової політики в сфері захисту інформації з обмеженим доступом.</p> <p>Наголос робиться на розвитку професійного самовдосконалення, творчого мислення та пошуку нестандартних управлінських рішень у сфері захисту інформації з обмеженим доступом.</p> <p>Спеціалізація: «Організація захисту інформації з обмеженим доступом» спрямована на формування повного комплексу фахових компетенцій, що дають можливість випускникам здійснювати менеджмент державних та приватних систем забезпечення обігу інформації з обмеженим доступом.</p>
	<i>Орієнтація програми</i>	<p>Програма пропонує комплексний підхід до управління сучасним підприємством та реалізує це через навчання та практичну підготовку. Освітня програма, орієнтується на сучасні наукові дослідження в галузі організації захисту інформації з обмеженим доступом, враховує специфіку роботи підприємств різних форм власності у цьому напрямі; базується на апробованих практичних результатах із врахуванням сьогодишнього стану та перспектив розвитку сфери захисту інформації з обмеженим доступом, орієнтує на подальшу професійну та наукову кар'єру.</p>
	<i>Особливості програми</i>	<p>Програма розвиває перспективи професійної підготовки фахівців в менеджменті з урахуванням специфічних особливостей функціонування підприємств, установ, організацій різних форм власності, які провадять діяльність пов'язану з обігом різних видів інформації з обмеженим доступом (від найпоширеніших потреб у захисті персональних даних працівників та конфіденційної інформації фірми, комерційної, банківської таємниці до забезпечення режиму секретності на підприємствах, в установах і організаціях, що провадять діяльність пов'язану з держаною таємницею).</p>
С	Працевлаштування та продовження освіти	
	<i>Працевлаштування</i>	<p>Робочі місця на підприємствах різних форм власності на посадах: начальника режимно-секретного підрозділу (управління, самостійного відділу), який класифікується як «Керівники інших основних підрозділів в інших сферах діяльності»; начальника відділу (в складі управління) підвідділу, сектору (в складі самостійного відділу) з режиму секретності та начальник відділу (в складі управління) підвідділу, сектору (в складі самостійного відділу) з організації захисту інформації, який класифікується як «Керівники інших функціональних підрозділів»; менеджерів підприємства, який класифікується, як: «Професіонал із організації захисту інформації з обмеженим доступом».</p> <p>Магістр готується для роботи підприємств, установ, організацій різних форм власності, які провадять діяльність пов'язану з обігом різних видів інформації з обмеженим доступом.</p>
	<i>Академічні права випускників</i>	<p>Можливість продовжувати навчання за програмою третього освітньо-наукового рівня вищої освіти – доктора філософії. Набуття додаткових кваліфікацій в системі післядипломної освіти</p>
Д	Стиль викладання та методика навчання	
	<i>Підходи до викладання та навчання</i>	<p>Студентоцентроване, проблемно-орієнтоване навчання, ініціативне самонавчання. Лекційні заняття мають інтерактивний</p>

		науково-пізнавальний характер. Практичні проводяться в малих групах, поширеними є кейс-метод, ситуаційні завдання, тренінги, дискусії, ділові ігри, використання сучасних професійних програмних засобів, індивідуальних занять, проходження практики.
	<i>Система оцінювання</i>	Накопичувальна модульно-рейтингова система, що передбачає оцінювання студентів за усіма видами аудиторної та поза аудиторної (самостійної, індивідуальної) навчальної діяльності, спрямовані на опанування навчального матеріалу з освітньої програми: поточний контроль, модульний, підсумковий контроль, письмові та усні экзамени, тестування, реферати, презентації, проходження навчальних та виробничих практик, написання курсових робіт, підготовка та захист магістерської дипломної роботи, комплексні кваліфікаційні экзамени з фаху. Рівень досягнутих результатів навчання вимірюється у трьох системах оцінювання: рейтингова шкала або 100-бальна, національна та шкала ЄКТС. Критерії та методи оцінювання розробляються кафедрами й визначаються в програмах навчальних дисциплін, практичної підготовки та атестації.
ОБСЯГ КРЕДИТІВ ЄКТС, НЕОБХІДНИЙ ДЛЯ ЗДОБУТТЯ ВІДПОВІДНОГО СТУПЕНЯ ВИЩОЇ ОСВІТИ		
		Освітньо-професійна програма, 90 кредитів ЄКТС, 1 рік 6 місяців. Основні предмети – менеджмент організацій, антикризовий менеджмент, кадрова політика в сфері захисту інформації з обмеженим доступом, спеціалізовані – охорона державної таємниці, охорона персональних даних, організація та управління службою захисту інформації, конкурентна розвідка, комплексні системи захисту інформації, правові засади охорони банківської таємниці, міжнародні стандарти захисту інформації, охорона комерційної таємниці. Програма передбачає такі компоненти: - Цикл загальної підготовки (13 кредитів ЄКТС, 390 год. – 14,4%); - Цикл професійної підготовки (20 кредитів ЄКТС, 990 год.; разом із написанням курсової роботи, проходження практики – 22,2%); - Вибіркові навчальні дисципліни (57 ЄКТС, 1320 год., із яких: спеціалізація – 33 кредити ЄКТС (36,6%), дисципліни вільного вибору студента – 24 кредити ЄКТС (26,8%).
Е	ПЕРЕЛІК КОМПЕТЕНТНОСТЕЙ ВИПУСКНИКА	
	Інтегральна компетентність	Здатність розв'язувати складні задачі і проблеми у сфері менеджменту або у процесі навчання, що передбачають проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.
	<i>Загальні компетентності</i>	<i>Аналіз та синтез.</i> Здатність аналізувати та структурувати проблему підприємства та приймати оптимальні управлінські рішення на основі логічних аргументів та перевірених фактів з діяльності пов'язаної з обігом різних видів інформації з обмеженим доступом. Здатність аналізувати основні проблеми організації захисту інформації з обмеженим доступом, організувати власну діяльність з огляду на досягнення науки та

		<p>з урахуванням динамічних змін, що відбуваються у сфері національної безпеки.</p> <p><i>Гнучкість мислення.</i> Здатність застосовувати сукупність знань для розуміння та розв'язання складних проблем та задач зі збереженням критичного ставлення до сталих наукових концепцій.</p> <p><i>Адаптивність.</i> Здатність розуміти та вирішувати нові проблеми інноваційного менеджменту під впливом змін у середовищі функціонування підприємств.</p> <p><i>Комунікативна здатність, робота в команді.</i> Уміння вести дискусію й навчати співробітників новим методам організації захисту інформації з обмеженим доступом; здатність до ділових комунікацій у сфері організації захисту інформації з обмеженим доступом, знання основ ділового спілкування, навички роботи в команді</p> <p><i>Здатність до навчання та готовність підвищувати рівень своїх знань.</i> Знання дієвих загальнодержавних інформаційних систем, насамперед, у соціальних сферах охорони здоров'я, освіти, науки, культури, охорони довкілля; уміння вести дискусію й навчати співробітників новим методам організації захисту інформації з обмеженим доступом;</p> <p><i>Знання ділової іноземної мови.</i> Вільне володіння, читання, аудіювання, письмо іноземною мовою, що дозволяє працювати англійською мовою, наприклад, якщо вона є іноземною.</p> <p><i>Здатність до наукової діяльності.</i> Здатність використовувати наукову організацію управлінської праці співробітників, задіяних у системі організації захисту інформації з обмеженим доступом.</p>
	<p><i>Фахові компетентності</i></p>	<p><i>Глибокі знання та розуміння.</i> Детальні знання та розуміння систем захисту інформації з обмеженим доступом та порядку реалізації заходів захисту. Здатність моделювати процеси у сфері захисту інформації з обмеженим доступом та поведінку їх учасників, прогнозувати подальший розвиток процесів і явищ, пов'язаних з можливим витоком інформації та протиправною діяльністю у цій сфері окремих організацій, груп та осіб, застосовувати ефективні методи і прийоми вироблення і прийняття управлінських рішень.</p> <p><i>Експериментальні навички.</i> Здатність до проектування, розробки та впровадження комплексної системи захисту інформації з обмеженим доступом на підприємстві, установі, організації. Здатність формулювати, аналізувати та синтезувати вирішення широкого кола загальних проблем і задач (завдань) з організації та захисту інформації з обмеженим доступом на підприємстві в установі, організації.</p> <p><i>Здатність до наукової діяльності.</i> Здатність досліджувати та аналізувати обставини, що призводять до витоку інформації з обмеженим доступом, економічні, правові, соціальні, інженерно-технічні та побутові аспекти проблеми.</p> <p><i>Навички оцінювання.</i> Здатність до комплексного аналізу актуальних проблем у сфері захисту інформації з обмеженим доступом та до їх розв'язання методами наукового пошуку.</p> <p><i>Професійна ерудиція.</i> Здатність навчати співробітників новим методам організації захисту інформації з обмеженим доступом.</p>

F	<p><i>Програмні результати навчання.</i></p>	<p>Успішне завершення програми передбачає, що здобувач вищої освіти демонструє:</p> <p><i>Знання та розуміння предметної області:</i> спеціалізовані концептуальні знання з організації та розроблення комплексної системи захисту інформації з обмеженим доступом та формування системи суб'єктів захисту інформації з обмеженим доступом установ, підприємств, організацій. Спеціалізовані концептуальні знання про принципи моніторингу, протидію загрозам конфіденційності, цілісності, доступності інформації з обмеженим доступом і уміння їх використовувати. Спеціалізовані концептуальні знання для проведення заходів захисту інформації, що обробляється в базах персональних даних. Спеціалізовані концептуальні знання для формування системи (органів, підрозділів), що забезпечує захист інформації з обмеженим доступом підприємств, установ організацій. Розв'язання складних задач зі створення та документального оформлення баз персональних даних на підприємствах, установах та організаціях різних формах власності.</p> <p><i>Практичні уміння та навички з предметної області:</i></p> <p>Здатність організовувати та спрямовувати діяльність фахівців з режиму секретності. Здатність розробляти та впроваджувати заходи із охорони державної таємниці та режиму секретності, самостійно та у взаємодії з контролюючими органами. Здатність роботи з секретними документами, їх документування, облік, розмноження, знищення, експертизу цінності, передавання на архівне зберігання технічної документації, чинні ДСТУ, МСТ, ЄСКД та інші нормативи з питань розробки та оформлення секретної проектно-конструкторської та текстової експлуатаційно-технологічної документації. Здатність до формування відомчої нормативної бази щодо обробки інформації з обмеженим доступом. Здатність використовувати професійно профільовані знання із організації захисту інформації з обмеженим доступом для моделювання загроз та розробки заходів протидії їм. Здатність до системного аналізу стану захищеності інформації з обмеженим доступом на підприємстві, в установі, організації. Здатність до комплексного аналізу актуальних проблем у сфері організації захисту інформації з обмеженим доступом та до їх розв'язання методами наукового пошуку (самостійно та у складі груп). Здатність до вибору адекватних форм і методів протидії конкурентної розвідки, використання легальних методів отримання інформації. Здатність до застосування заходів захисту банківської таємниці в банківській установі. Здатність до проведення заходів із захисту банківської таємниці та організовувати протидію загрозам протиправного отримання банківської інформації. Здатність забезпечувати організацію захисту інформації з обмеженим доступом в установі, організації на основі міжнародних стандартів безпеки (ISO/IEC). Здатність оцінювати системи безпеки на предмет відповідності міжнародним стандартам (ISO/IEC). Спеціалізовані концептуальні знання зі змісту та основних ознак комерційної таємниці, способи, методи, принципи організації охорони комерційної таємниці; Спеціалізовані концептуальні знання для</p>
---	--	--

	організаційно-правового забезпечення охорони комерційної таємниці.
<i>Гарант освітньої програми</i>	доктор історичних наук, професор, завідувач кафедри організації захисту інформації з обмеженим доступом Гуз Анатолій Михайлович

I. Загальна характеристика освітньої програми:

№ з/п	Назва показника	Значення показника
1. Показники освітньої програми (у кредитах ЄКТС/годинах)		
1.1.	Загальний обсяг за весь термін навчання	90/2700
1.2.	Обсяг нормативної (обов'язкової) складової	33/990
1.3.	Обсяг вибіркової складової, у тому числі для:	57/1710
1.3.1.	спеціалізації	33/990
1.3.2.	вільного вибору здобувачів освіти	24/720
1.4.	Обсяг циклу загальної (соціально-гуманітарної, фундаментальної) підготовки	13/390
1.5.	Обсяг циклу професійної (фахової) підготовки	53/1590
2. Показники навчального навантаження здобувачів освіти (у кредитах ЄКТС/годинах)		
2.1.	Обсяг по рокам навчання	
2.1.1.	1 рік навчання	60/1800
2.1.2.	2 рік навчання	30/900
2.2.	Тижневе навантаження	
2.2.1.	максимальне	1,75 кр/52,5 г
2.2.2.	мінімальне	1,5кр/45 г
3. Показник співвідношення між аудиторними годинами і годинами самостійної роботи (у годинах) здобувачів освіти		
3.1.	Обсяг аудиторних годин	956
3.2.	Обсяг самостійної роботи	1744
4. Загальні показники навчальних дисциплін (спецкурсів), практичної підготовки, атестації		
4.1.	Мінімальний обсяг навчальної дисципліни (спецкурсу)	3/90
4.2.	Орієнтовна кількість навчальних дисциплін (спецкурсів)/із них за вільним вибором здобувачів освіти	15/*
4.3.	Вид практичної підготовки (<i>тривалість у тижнях</i>)	
4.3.1.	Науково-дослідна практика	6
4.4.	Форма та назва атестації (<i>тривалість підготовки до неї в днях</i>)	
4.4.1.	Комплексний екзамен із менеджменту організацій в звичайних та кризових умовах	5 днів
4.4.2.	Комплексний екзамен із організації захисту інформації з обмеженим доступом	5 днів
5. Каталоги навчальних дисциплін (спецкурсів) нормативної (обов'язкової) складової освітньої програми (<i>назва дисципліни (спецкурсу), номер додатка до Схеми, р/н</i>)		
5.1.	Методологія наукових досліджень (<i>додаток 5.1, р/н 22/761-346</i>)	

5.2.	Теорія прийняття рішень (додаток 5.2, р/н 22/761-347)
5.3.	Іноземна мова (професійного спрямування) (додаток 5.3, р/н 22/761-348)
5.4.	Менеджмент організацій (додаток 5.4, р/н 22/761-349)
5.5.	Антикризовий менеджмент (додаток 5.5, р/н 22/761-350)
5.6.	Кадрова політика в сфері захисту інформації з обмеженим доступом (додаток 5.6, р/н 22/761-351)
5.7.	Науково-дослідна практика (додаток 5.7, р/н 22/761-352)
6. Каталоги навчальних дисциплін (спецкурсів), що утворюють спеціалізацію освітньої програми (назва дисципліни (спецкурсу), номер додатка до Схеми, р/н)	
6.1.	Охорона державної таємниці (додаток 6.1, р/н 22/761-353)
6.2.	Охорона персональних даних (додаток 6.2, р/н 22/761-354)
6.3.	Організація та управління службою захисту інформації (додаток 6.3, р/н 22/761-355)
6.4.	Конкурентна розвідка (додаток 6.4, р/н 22/761-356)
6.5.	Комплексні системи захисту інформації (додаток №6.5, р/н 22/761-357)
6.6.	Правові засади охорони банківської таємниці (додаток 6.6, р/н 22/761-358)
6.7.	Міжнародні стандарти захисту інформації (додаток 6.7, р/н 22/761-359)
6.8.	Охорона комерційної таємниці (додаток 6.8, р/н 22/761-360)

* Примітка: на дисципліни вільного вибору студентів виділено 24 кредити. Остаточна кількість дисциплін залежатиме від вибору здобувачів вищої освіти.

НОРМАТИВНИЙ ЗМІСТ ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ, СФОРМУЛЬОВАНИЙ У ТЕРМІНАХ РЕЗУЛЬТАТІВ НАВЧАННЯ

1. Критично осмислювати, вибирати та використовувати необхідний науковий, методичний і аналітичний інструментарій для управління у непередбачуваних умовах.
2. Ідентифікувати проблеми в організації та обґартовувати методи їх вирішення
3. Проектувати ефективні системи управління організаціями.
4. Обґрунтовувати та управляти проектами, генерувати підприємницькі ідеї.
5. Планувати діяльність організації в стратегічному та тактичному розрізі.
6. Мати навички прийняття, обґрунтування та забезпечення реалізації управлінських рішень в непередбачуваних умовах, враховуючи вимоги чинного законодавства, етичні міркування та соціальну відповідальність.
7. Організовувати та здійснювати ефективні комунікації всередині колективу, з представниками різних професійних груп та в міжнародному контексті.
8. Застосовувати спеціальне програмне забезпечення та інформаційні системи для вирішення задач управління організацією.
9. Вміти спілкуватися у професійних і наукових колах державною та іноземною мовами.
10. Демонструвати лідерські навички та вміння працювати в команді, взаємодіяти з людьми, впливати на їх поведінку для вирішення професійних задач.
11. Забезпечувати особистий професійний розвиток та планування власного часу.

II. Співвідношення між компетентностями, що визначені освітньою програмою, та результатами навчання

2.1. Перелік компетентностей, визначених освітньою програмою (далі – програмні компетентності), та їх відповідність компетентностям за Національною рамкою кваліфікацій (далі – НРК):

Класифікація компетентностей за НРК		Знання	Уміння	Комунікація	Автономність та відповідальність	
1. Загальні програмні компетентності (далі – ЗГ)						
№ з/п	Шифр	Зміст				
1.1	ЗГ-01	<p><i>Аналіз та синтез.</i> Здатність аналізувати та структурувати проблему підприємства та приймати оптимальні управлінські рішення на основі логічних аргументів та перевірених фактів з діяльності пов'язаної з обігом різних видів інформації з обмеженим доступом. Здатність аналізувати основні проблеми організації захисту інформації з обмеженим доступом, організувати власну діяльність з огляду на досягнення науки та з урахуванням динамічних змін, що відбуваються у сфері національної безпеки.</p>	Організаційних структур управління.	Володіти специфікою відповідальності в менеджменті державних підприємств, установ і організацій.	Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем менеджменту захисту інформації з обмеженим доступом на підприємстві та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування
			Методів менеджменту підприємств, установ і організацій, їх класифікації.	Адаптувати методи управління до умов функціонування великих колективів і багатонаціональних корпорацій.	Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем менеджменту захисту інформації з обмеженим доступом на підприємстві та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування
			Загальних методів та критеріїв прийняття рішень, основи моделювання в теорії прийняття рішень, про методи подолання невизначеності в процесі прийняття рішень, принципи вирішення задач оптимізації при прийнятті рішень, основи застосування евристичних підходів до прийняття рішень.	На основі отриманих знань вибирати потрібні методи математичного моделювання з теорії прийняття рішень, визначати і розробляти заходи з прийняття рішень в умовах неповної інформаційної визначеності, комбінувати методи з теорії прийняття рішень, проводити оптимізацію При прийнятті конкретних рішень використовувати сучасні технології та методи створення інтелектуальних систем керування та підтримки прийняття рішень.	Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем менеджменту захисту інформації з обмеженим доступом на підприємстві та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування
				Визначати потребу підприємств у ресурсному забезпеченні та організувати їх оптимальне поєднання та взаємодію.	Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем менеджменту захисту інформації з обмеженим доступом на підприємстві та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування

				Розробляти достатню кількість альтернативних варіантів рішень, оцінювати їх ефективність та документально оформляти управлінське рішення.	Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем менеджменту захисту інформації з обмеженим доступом на підприємстві та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування
1.2	ЗГ-02	<i>Гнучкість мислення.</i> Здатність застосовувати сукупність знань для розуміння та розв'язання складних проблем та задач зі збереженням критичного ставлення до сталих наукових концепцій.	Основних методологічних положень та теоретичних методів дослідження систем управління підприємствами, установами і організаціями.	Використовувати методологічні положення дослідження систем управління підприємствами, установами, організаціями.	Зрозуміле і недвозначне донесення власних висновків, а також знань та пояснень, що їх обґрунтовують, до керівників підприємств, установ і організацій, а також взаємодіючих структур	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування
			Сучасних наукових концепцій в менеджменті.	Обирати необхідну для вирішення проблем інформацію на базі власних знань, аналізувати отриману інформацію, окремі її елементи, висловлювати припущення, гіпотези та робити певні висновки на основі аналізу фактів.	Зрозуміле і недвозначне донесення власних висновків, а також знань та пояснень, що їх обґрунтовують, до керівників підприємств, установ і організацій, а також взаємодіючих структур.	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування.
1.3	ЗГ-03	<i>Адаптивність.</i> Здатність розуміти та вирішувати нові проблеми інноваційного менеджменту під впливом змін у середовищі функціонування підприємств.	Функцій менеджменту державних підприємств, установ і організацій, їх класифікації.	Здійснювати класифікацію і застосовувати основні та загальні функції менеджменту державних підприємств, установ і організацій.	Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем інноваційного менеджменту на підприємстві та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування.
			Положень інноваційного менеджменту державних підприємств, установ і організацій.	Володіти специфікою відповідальності в менеджменті державних підприємств, установ і організацій;	Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем інноваційного менеджменту на підприємстві та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування.
				Визначати оптимальну інфраструктуру для організації діяльності підприємства.	Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем інноваційного менеджменту та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування
1.4	ЗГ-04	<i>Комунікативна здатність, робота в команді.</i> Уміння вести дискусію й навчати співробітників	Діяльності підприємства, стратегію і тактику її здійснення; планів розвитку, впровадження відповідної системи моніторингу й контролю.	Володіти сучасними підходами до моніторингу і впровадження нововведень в організації; знаходити та оцінювати нові ринкові можливості та формулювати бізнес ідеї.	Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем навчання співробітників підприємства, діловим комунікаціям та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування.

		новим методам організації захисту інформації з обмеженим доступом; здатність до ділових комунікацій у сфері організації захисту інформації з обмеженим доступом, знання основ ділового спілкування, навички роботи в команді.	Основ бізнесу.	Використовувати сучасні технології менеджменту та управляти бізнес-процесами підприємств.	Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем навчання співробітників підприємства, діловим комунікаціям та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування.
			Оптимальної структури підприємства.	Прогнозувати, проектувати та моделювати оптимальну структуру організації та її підсистем.	Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем навчання співробітників підприємства, діловим комунікаціям та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування
			Основ ділового спілкування, навички роботи в команді.	Демонструвати навички поєднання усіх видів ресурсів, організування колективної праці по досягненню місії організації.	Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем навчання співробітників підприємства, діловим комунікаціям та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування
			Основні поняття антикризового менеджменту та його системні характеристики.	Виявляти кризові ситуації.	Зрозуміле і недвозначне донесення власних висновків, а також знань та пояснень з антикризового менеджменту до фахівців і нефахівців, зокрема до осіб, які навчаються.	Управління комплексними діями або проектами, відповідальність за прийняття рішень у непередбачуваних умовах при організації роботи на підприємствах, установах, організаціях.
			Види діагностики кризових ситуацій у сучасному менеджменті.	Обирати методи діагностики кризи.	Зрозуміле і недвозначне донесення власних висновків, а також знань та пояснень з антикризового менеджменту до фахівців і нефахівців, зокрема до осіб, які навчаються.	Управління комплексними діями або проектами, відповідальність за прийняття рішень у непередбачуваних умовах при організації роботи на підприємствах, установах, організаціях.
			Основних доміант антикризового менеджменту; система критеріїв оцінювання розвитку кризової ситуації; кадрова політика системи антикризового управління.	Досліджувати причини настання кризових ситуацій на підприємствах зв'язку та сфери інформатизації залежно від його життєвого циклу; застосовувати аналітичні показники для оцінювання глибини кризи.	Зрозуміле і недвозначне донесення власних висновків, а також знань та пояснень з антикризового менеджменту до фахівців і нефахівців, зокрема до осіб, які навчаються.	Управління комплексними діями або проектами, відповідальність за прийняття рішень у непередбачуваних умовах при організації роботи на підприємствах, установах, організаціях.
1.5	ЗГ-05	<i>Здатність до навчання та готовність підвищувати рівень своїх знань.</i>	Заходів реалізації кадрової політики в залежності від виду управління та характеру ситуації конкретного суб'єкту господарювання із захисту інформації з обмеженим доступом.	Визначати завдання, види, зміст, організаційно-правові основи, принципи, етапи, характеристики та критерії оцінки, а також базові навички, на засадах аналізу та узагальнення сучасних методів і технологій, з організації заходів реалізації кадрової	Зрозуміле і недвозначне донесення власних висновків, а також знань та пояснень функціонування загальнодержавних інформаційних систем до осіб, які навчаються.	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування.

		Знання дієвих загальнодержавних інформаційних систем, насамперед, у соціальних сферах охорони здоров'я, освіти, науки, культури, охорони довкілля; уміння вести дискусію й навчати співробітників новим методам організації захисту інформації з обмеженим доступом.	Структури та змісту морально-етичних компонентів у менеджменті державних підприємств, установ і організацій; положень моральної культури співробітника підприємства, установи, організації; - основних норм і правил ділового етикету в менеджменті державних підприємств, установ і організацій.	політики в залежності від виду управління та характеру ситуації конкретного суб'єкту господарювання із захисту інформації з обмеженим доступом.		
1.6	ЗГ-06	Знання ділової іноземної мови. Вільне володіння, читання, аудіювання, письмо іноземною мовою, що дозволяє працювати англійською мовою, наприклад, якщо вона є іноземною.	Функціональної лексики англійської мови з тематики, що вивчається, для її подальшого вживання в усному та письмовому мовленні та при перекладі текстів за фахом; іншомовних особливостей ділового листування: лексика, граматики, синтаксис, діловий етикет, культурологічний аспект та принципи складання ділових листів.	Володіти навичками усної комунікації та застосовувати їх для спілкування на теми загального та професійного спілкування; Розуміти усне (монологічне й діалогічне) мовлення за темами загального та професійного характеру.	Чітке формулювання власних обґрунтованих висновків іноземною мовою та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування.
1.7	ЗГ-07	Здатність до наукової діяльності. Здатність використовувати наукову організацію управлінської праці співробітників, задіяних у системі організації захисту інформації з обмеженим доступом.	Принципів наукової організації праці на підприємстві установі в організації. Методології проведення науково-дослідної роботи на підприємствах, установах, організаціях з проблем організації захисту інформації з обмеженим доступом; методика самостійної дослідницької роботи.	Застосовувати дослідницькі методи для розв'язання практичних і теоретичних питань майбутньої професійної діяльності. Проводити науково-дослідну роботу в академічних та спеціалізованих інститутах, провідних компаніях з проблем організації захисту інформації з обмеженим доступом; здійснювати комплексний аналіз актуальних проблем у сфері організації захисту інформації з обмеженим доступом та до їх розв'язання методами наукового пошуку (самостійно та у складі груп); досліджувати та аналізувати обставини, що призводять до витoku інформації з обмеженим доступом, економічні, правові, соціальні, інженерно-технічні та побутові аспекти проблеми.	Зрозуміле і недвозначне донесення принципів наукової організації праці до осіб, які навчаються. Зрозуміле і недвозначне донесення принципів наукової організації праці до осіб, які навчаються.	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування Відповідальність за розвиток професійного знання в практик, оцінку стратегічного розвитку команди.

			Сутності сучасних наукових концепцій менеджменту державних підприємств, установ і організацій.	Застосовувати принципи менеджменту державних підприємств, установ і організацій.	Зрозуміле і недвозначне донесення принципів наукової організації праці до осіб, які навчаються.	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування.
2. Спеціальні (фахові) програмні компетентності (далі – СФ)						
2.1	СФ-01	<i>Глибокі знання та розуміння.</i> Детальні знання та розуміння систем захисту інформації з обмеженим доступом та порядку реалізації заходів захисту. Здатність моделювати процеси у сфері захисту інформації з обмеженим доступом та поведінку їх учасників, прогнозувати подальший розвиток процесів і явищ, пов'язаних з можливим витоком інформації та протиправною діяльністю у цій сфері окремих організацій, груп та осіб, застосовувати ефективні методи і прийоми вироблення і прийняття управлінських рішень.	<p>Положень чинного законодавства України в частині, що стосується захисту інформації з обмеженим доступом, комерційної, банківської таємниці, а також міжнародних угод, державні та відомчі нормативні акти з питань забезпечення інформаційної безпеки.</p> <p>Організаційно-технічних заходів для забезпечення захисту інформації з обмеженим доступом на всіх етапах виконання робіт, змісту та технологію секретного діловодства, принципів та порядку оформлення облікової, супровідної та іншої документації на виробі спецвиробів (техніки).</p> <p>Основних положень законодавства та організаційно-правові заходи і суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, в Україні; сутність державної політики щодо державної таємниці; головні суб'єкти охорони державної таємниці; компетенцію органів державної влади, органів місцевого самоврядування та їх посадових осіб, а також керівників підприємств, установ, організацій у сфері охорони державної таємниці; правовий статус та компетенцію СБ України, як спеціально уповноваженого органу у сфері охорони державної таємниці; правові режими у сфері охорони державної таємниці; порядок віднесення інформації до державної таємниці; механізм засекречування</p>	<p>Формувати відомчу нормативну базу щодо обробки інформації з обмеженим доступом; проводити заходи із захисту комерційної та банківської таємниці та організувати протидію загрозам протиправного отримання цих видів таємної інформації.</p> <p>На підставі обґрунтованих пропозицій фахівців структурних підрозділів організації, підприємства і разом з ними формувати номенклатуру посад працівників, що підлягають оформленню на допуск до інформації зі ступенем секретності, за участю кадрових служб оформляти документи на допуск працівників до цієї інформації; контролювати стан режиму секретності в режимних підрозділах організації, підприємства, на робочих місцях виконавців.</p> <p>Розв'язувати складні спеціалізовані задачі та практичні проблеми у менеджменті, що безпосередньо пов'язані із охороною державної таємниці.</p>	<p>Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем захисту інформації з обмеженим доступом на підприємстві та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.</p> <p>Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем захисту інформації з обмеженим доступом на підприємстві та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.</p> <p>Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем захисту інформації з обмеженим доступом на підприємстві та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.</p>	<p>Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування.</p> <p>Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування.</p> <p>Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування.</p>

			та розсекречування матеріальних носіїв секретної інформації; порядок допуску та доступу осіб до державної таємниці; зміст охорони державної таємниці під час міжнародного співробітництва; зміст попереджувально-профілактичної роботи у сфері охорони державної таємниці; види та зміст юридичної відповідальності за порушення законодавства про державну таємницю; особливості організації технічного захисту секретної інформації; процедуру організації менеджменту, що безпосередньо пов'язаний із захистом державної таємниці.			
			Основних положень законодавства та організаційно-правових заходів і суспільних відносин, пов'язаних з віднесенням інформації до комерційної таємниці, принципів, міжнародного досвіду і новітніх технологій оптимізації роботи щодо охорони комерційної таємниці; механізмів засекречування, розсекречування її матеріальних носіїв.	Застосовувати організаційні форми режиму і процедури розкриття охорони комерційної таємниці, виявляти, попереджувати та припиняти правопорушень у цій сфері; моделювати явища та процесів, які зумовлюють загрози витоку конфіденційної інформації; розробка проектів нормативних документів, особливостей управління системою охорони комерційної таємниці з метою захисту економічної безпеки суб'єктів господарювання.	Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем захисту інформації з обмеженим доступом на підприємстві та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування.
2.2	СФ-02	<i>Експериментальні навички.</i> Здатність до проектування, розробки та впровадження комплексної системи захисту інформації з обмеженим доступом на підприємстві, установі, організації. Здатність формулювати, аналізувати та синтезувати вирішення широкого кола загальних проблем і задач (завдань) з організації та захисту інформації з обмеженим доступом на	Знання з організації та розроблення комплексної системи захисту інформації з обмеженим доступом та формування системи суб'єктів захисту інформації з обмеженим доступом установ, підприємств, організацій.	Застосовувати професійно-профільовані знання із організації захисту інформації з обмеженим доступом для моделювання загроз та розробки заходів протидії їм. аналізувати стан захищеності інформації з обмеженим доступом на підприємстві, в установі, організації.	Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем проектування, розробки та впровадження комплексної системи захисту інформації з обмеженим доступом на підприємстві та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування.
			Чинних ДСТУ, міжнародних стандартів безпеки (ISO/IEC), ЄСКД та інші нормативи, які регулюють питання організації захисту інформації з обмеженим доступом.	Роботи з секретними документами, їх документування, облік, розмноження, знищення, експертизу цінності, передавання на архівне зберігання технічної документації, чинні ДСТУ, МСТ, ЄСКД та інші нормативи з питань розробки та оформлення секретної проектно-конструкторської та текстової експлуатаційно-технологічної документації; забезпечувати організацію захисту інформації з обмеженим доступом в установі, організації на основі міжнародних стандартів безпеки (ISO/IEC), оцінювати	Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем проектування, розробки та впровадження комплексної системи захисту інформації з обмеженим доступом на підприємстві та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.	прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування.

		<p>підприємстві в установі, організації.</p>		<p>системи безпеки на предмет відповідності міжнародним стандартам (ISO/IEC).</p>		
		<p>Організації та оснащення системи охорони організації, підприємства, їх режимних приміщень.</p>	<p>Організовувати та спрямовувати діяльність фахівців з режиму секретності; розробляти та впроваджувати заходи із охорони державної таємниці та режиму секретності, самостійно та у взаємодії з контролюючими органами; розробляти та впроваджувати заходи для забезпечення режиму секретності в разі здійснення організацією, підприємством науково-технічних, торговельно-економічних та інших міжнародних зв'язків, в тому числі під час відвідування організації, підприємства іноземцями.</p>	<p>Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем проектування, розробки та впровадження комплексної системи захисту інформації з обмеженим доступом на підприємстві та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.</p>		<p>Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування</p>
		<p>Нормативно-правової бази України та міжнародних стандартів щодо сфери захисту інформації та керування ними під час роботи по створенню комплексних систем захисту інформації.</p>	<p>Застосовувати сучасні методи, засоби та заходи криптографічного й технічного захисту інформації, технічні засоби охорони та контролю об'єктів інформаційної діяльності; організовувати заходи по створенню КСЗІ в ІТС та КТЗІ на ОІД, розробляти план захисту інформації в ІТС, розробляти технічне завдання на побудову КСЗІ в ІТС, створювати службу захисту інформації в ІТС, проводити експлуатацію КСЗІ в ІТС, проводити науково-практичні дослідження КСЗІ та КТЗІ.</p>	<p>Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем проектування, розробки та впровадження комплексної системи захисту інформації з обмеженим доступом на підприємстві та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.</p>		<p>Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування.</p>
		<p>Концептуальних положень різних галузей національного права, які регламентують режим охорони банківської таємниці, усвідомлення їх прогальності, колізійності тощо на основі критичного ставлення до чинного національного законодавства і міжнародних правових актів у сфері банківської таємниці.</p>	<p>Розв'язання складних задач правової охорони банківської таємниці, що потребують інтеграції знань з різних галузей, в невизначених умовах безпеки банківської установи.</p>	<p>Чітке формулювання власних обґрунтованих висновків щодо правового вирішення проблем охорони банківської таємниці та однозначне донесення їх до фахівців і нефахівців, зокрема до осіб, які навчаються.</p>		<p>Прийняття рішень у складних і непередбачуваних умовах банківської діяльності, що потребує інноваційної та прогностичної діяльності; власна відповідальність за професійний розвиток колективу, стимулювання його до отримання нових знань у сфері охорони банківської таємниці.</p>
		<p>Концептуальних положень національного і міжнародного права, які регламентують режим охорони банківської таємниці в Україні і світі; усвідомлення проблем у сфері персональних даних на основі критичного ставлення до наявних механізмів їхньої охорони.</p>	<p>Розв'язання складних задач охорони персональних даних, що потребують комплексних знань з гуманітарних і технічних наук, у динамічному інформаційному середовищі сучасного суспільства.</p>	<p>Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем охорони персональних даних та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.</p>		<p>Прийняття рішень щодо охорони персональних даних у складних і непередбачуваних інформаційних умовах життя суспільства, що потребує інноваційної та прогностичної діяльності; власна відповідальність за професійний розвиток колективу, стимулювання його до отримання нових</p>

						знань у сфері охорони персональних даних.
2.3	СФ-03	<i>Здатність до наукової діяльності.</i> Здатність досліджувати та аналізувати обставини, що призводять до витоку інформації з обмеженим доступом, економічні, правові, соціальні, інженерно-технічні та побутові аспекти проблеми.	Тематики робіт та режимність підрозділів, кооперацію організації, підприємства, правила проведення службових розслідувань. Принципів моніторингу, протидії загрозам конфіденційності, цілісності, доступності інформації з обмеженим доступом і уміння їх використовувати.	Аналізувати актуальні проблеми у сфері організації захисту інформації з обмеженим доступом та їх розв'язання методами наукового пошуку (самостійно та у складі груп); брати безпосередню участь у проведенні службових розслідувань за фактами втрати та розголошення інформації з обмеженим доступом, а також за фактами порушення внутрішньооб'єктового та перепускного режиму. Розробляти та здійснювати конкретні заходи для запобігання розголошення та витоку незаконної модифікації та знищення інформаційних ресурсів різних суб'єктів інформаційної діяльності; вибирати адекватні форм і методів протидії конкурентній розвідці, використовувати легальні методи отримання інформації.	Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем наукової діяльності з питань захисту інформації з обмеженим доступом та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються. Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем наукової діяльності з питань захисту інформації з обмеженим доступом та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування. Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування
2.4	СФ-04	<i>Навички оцінювання.</i> Здатність до комплексного аналізу актуальних проблем у сфері захисту інформації з обмеженим доступом та до їх розв'язання методами наукового пошуку.	Напрямів науково-дослідної та дослідно-конструкторської роботи, номенклатуру секретних виробів організації, підприємства, їх тактико-технічні характеристики, які підлягають охороні. Заходів захисту інформації, що обробляється в базах персональних даних, зі створення та документального оформлення баз персональних даних на підприємствах, установах та організаціях різних формах власності. Організаційно-правових основ роботи конкурентної розвідки на підприємстві.	Вивчати та аналізувати окремі напрями виробничо-технічної, науково-дослідної, дослідно-конструкторської та іншої діяльності організації, підприємства з метою виявлення та закриття можливих каналів витоку інформації з обмеженим доступом; аналізувати, поширювати позитивний досвід роботи за результатами перевірок стану режиму секретності та іншими матеріалами, брати участь у проведенні навчання з метою підвищення кваліфікації працівників підрозділу, інструктажі працівників, допущених до секретних робіт, документів та виробів, у прийомі заліків з метою перевірки засвоєння ними відповідних вимог режиму секретності. Створювати та захищати відповідно до чинного законодавства бази персональних даних; здійснювати заходи для захисту інформації з обмеженим доступом під час її обробки засобами обчислювальної техніки. Визначати і характеризувати методологію інформаційно-аналітичної діяльності конкурентної розвідки; застосовувати інформаційно-аналітичні технології, які використовує в роботі конкурентної розвідки; створювати нові інформаційні продукти на	Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем комплексного захисту інформації з обмеженим доступом та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються. Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем комплексного захисту інформації з обмеженим доступом та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.	Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування. Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування.

				<p>основі аналітико-синтетичного опрацювання інформаційних матеріалів;</p> <ul style="list-style-type: none"> - використовувати методи конкурентної розвідки для збирання інформації з відкритих джерел; - формувати конкурентну стратегію інформаційної безпеки підприємства; <p>застосовувати способи використання наявних та перспективних інформаційних технологій для подальшого прогнозування результатів їх впровадження та вироблення управлінських рішень.</p>		
2.5	СФ-05	<p><i>Професійна ерудиція.</i></p> <p>Здатність навчати співробітників новим методам організації захисту інформації з обмеженим доступом.</p>	<p>Системи (органів, підрозділів), що забезпечує захист інформації з обмеженим доступом підприємств, установ організацій.</p>	<p>Організувати та провадити роботу покладену на підрозділ, забезпечувати виконання вимог керівних та інших документів з питань організації захисту інформації з обмеженим доступом; розробляти та здійснювати заходи для забезпечення перепускного і внутрішньооб'єктового режиму, охорони організації, підприємства; готувати необхідні матеріали для звіту та пропозиції з організації захисту інформації до плану роботи підрозділу.</p>	<p>Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем навчання співробітників щодо захисту інформації з обмеженим доступом та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.</p>	<p>Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування.</p>
			<p>Організаційно-технічних заходів для забезпечення захисту інформації з обмеженим доступом на всіх етапах виконання робіт, змісту та технологію секретного діловодства, принципів та порядку оформлення облікової, супровідної та іншої документації на виробі спецпродукції (техніки).</p>	<p>На підставі обґрунтованих пропозицій фахівців структурних підрозділів організації, підприємства і разом з ними формувати номенклатуру посад працівників, що підлягають оформленню на допуск до інформації зі ступенем секретності, за участю кадрових служб оформляти документи на допуск працівників до цієї інформації. контролювати стан режиму секретності в режимних підрозділах організації, підприємства, на робочих місцях виконавців.</p>	<p>Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем навчання співробітників щодо захисту інформації з обмеженим доступом та однозначне донесення їх до широкого кола осіб зокрема до тих, які навчаються.</p>	<p>Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування.</p>
			<p>Основних положення трудового законодавства, вимог з питань охорони праці та техніки безпеки, пожежної безпеки, внутрішньооб'єктового та перепускного режиму, трудовий</p>	<p>Здійснювати в підрозділах профілактичну роботу з усіма категоріями працівників з питань додержання вимог режиму секретності, під час роботи з інформацією з обмеженим доступом; вести облік режимних приміщень, в яких дозволено постійно або тимчасово зберігати вироби, контролювати порядок видання та використання бланків службових посвідчень (перепусток);</p>	<p>Чітке формулювання власних обґрунтованих висновків щодо вирішення проблем навчання співробітників щодо захисту інформації з обмеженим доступом та однозначне донесення їх до</p>	<p>Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування.</p>

			розпорядок, правила та засоби проведення профілактичної роботи.	вести діяльність з дотриманням вимог трудового та інформаційного законодавства.	широкого кола осіб зокрема до тих, які навчаються.	
--	--	--	---	---	--	--

2.2. Перелік результатів навчання та їх відповідність програмним компетентностям:

Шифри програмних компетентностей		ЗГ-01	ЗГ-02	ЗГ-03	ЗГ-04	ЗГ-05	ЗГ-06	ЗГ-07	СФ-01	СФ-02	СФ-03	СФ-04	СФ-05
Результати навчання (далі - РН)													
Шифр	Зміст												
РН-01	Спеціалізовані концептуальні знання з організації та розроблення комплексної системи захисту інформації з обмеженим доступом та формування системи суб`єктів захисту інформації з обмеженим доступом установ, підприємств, організацій.	+	+	-	+	+	-	+	+	+	-	+	-
РН-02	Спеціалізовані концептуальні знання про принципи моніторингу, протидію загрозам конфіденційності, цілісності, доступності інформації з обмеженим доступом і уміння їх використовувати.	+	+	-	+	+	-	+	+	+	-	+	-
РН-03	Спеціалізовані концептуальні знання для проведення заходів захисту інформації, що обробляється в базах персональних даних.	+	+	-	+	+	-	+	+	+	-	+	-
РН-04	Спеціалізовані концептуальні знання для формування системи (органів, підрозділів), що забезпечує захист інформації з обмеженим доступом підприємств, установ організацій.	+	+	-	+	+	-	+	+	+	-	+	-

PH-05	Розв'язання складних задач зі створення та документального оформлення баз персональних даних на підприємствах, установах та організаціях різних формах власності.	+	-	-	-	+	-	+	+	+	+	+	-
PH-06	Здатність організувати та спрямовувати діяльність фахівців з режиму секретності.	+	+	+	+	+	-	+	+	+	+	+	+
PH-07	Здатність розробляти та впроваджувати заходи із охорони державної таємниці та режиму секретності, самостійно та у взаємодії з контролюючими органами.	+	+	-	-	+	-	+	+	+	+	+	+
PH-08	Здатність роботи з секретними документами, їх документування, облік, розмноження, знищення, експертизу цінності, передавання на архівне зберігання технічної документації, чинні ДСТУ, МСТ, ЄСКД та інші нормативи з питань розробки та оформлення секретної проектно-конструкторської та текстової експлуатаційно-технологічної документації.	+	+	-	-	+	-	+	+	+	+	+	+
PH-09	Здатність до формування відомчої нормативної бази щодо обробки інформації з обмеженим доступом.	+	+	-	-	+	-	-	+	+	+	+	-

PH-10	Здатність використовувати професійно профільовані знання із організації захисту інформації з обмеженим доступом для моделювання загроз та розробки заходів протидії їм.	+	+	+	+	+	-	+	+	+	+	+	+
PH-11	Здатність до системного аналізу стану захищеності інформації з обмеженим доступом на підприємстві, в установі, організації.	+	+	+	+	+	-	+	+	+	+	+	+
PH-12	Здатність до комплексного аналізу актуальних проблем у сфері організації захисту інформації з обмеженим доступом та до їх розв'язання методами наукового пошуку (самостійно та у складі груп).	+	+	+	+	+	+	+	+	+	+	+	+
PH-13	Здатність до вибору адекватних форм і методів протидії конкурентної розвідки, використання легальних методів отримання інформації.	+	+	-	+	-	+	+	+	+	+	+	+
PH-14	Здатність до застосування заходів захисту банківської таємниці в банківській установі.	+	+	+	+	-	+	+	+	+	+	+	+
PH-15	Здатність до проведення заходів із захисту банківської таємниці та організувати протидію загрозам протиправного отримання банківської інформації.	+	+	+	+	-	+	-	+	-	-	+	+

PH-16	Здатність забезпечувати організацію захисту інформації з обмеженим доступом в установі, організації на основі міжнародних стандартів безпеки (ISO/IEC).	+	-	-	+	+	+	+	-	+	+	+	+
PH-17	Здатність оцінювати системи безпеки на предмет відповідності міжнародним стандартам (ISO/IEC). Спеціалізовані концептуальні знання зі змісту та основних ознак комерційної таємниці, способи, методи, принципи організації охорони комерційної таємниці; Спеціалізовані концептуальні знання для організаційно-правового забезпечення охорони комерційної таємниці.	+	+	-	+	+	+	+	+	-	+	+	-

Примітка: відповідність позначається символом «+», в іншому випадку символом «-».

2.3. Перелік навчальних дисциплін (спецкурсів) та їх відповідність результатам навчання:

Шифри результатів навчання компетентностей			PH-01	PH-02	PH-03	PH-04	PH-05	PH-06	PH-07	PH-08	PH-09	PH-10	PH-11	PH-12	PH-13	PH-14	PH-15	PH-16	PH-17	
№ з/п	Повна назва дисципліни	Шифр																		
Навчальні дисципліни (далі – НД)																				
1.	Методологія наукових досліджень	НД-01	-	-	-	-	-	-	-	-	-	+	+	+	-	-	-	-	-	-
2.	Теорія прийняття рішень	НД-02	-	-	-	+	-	-	-	-	-	+	+	+	-	-	-	-	-	-
3.	Іноземна мова (професійного спрямування)	НД-03	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	+	+	-
4.	Менеджмент організацій	НД-04	+	-	-	+	-	-	-	-	+	+	+	-	-	-	-	+	-	-
5.	Антикризовий менеджмент	НД-05	-	+	-	+	-	-	-	-	-	-	+	-	+	+	+	-	-	-
6.	Кадрова політика в сфері захисту інформації з обмеженим доступом	НД-06	+	+	-	-	-	-	-	-	-	+	+	+	-	-	-	-	-	-
7.	Науково-дослідна практика	НД-07	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
8.	Охорона державної таємниці	НД-08	+	+	-	+	-	+	+	+	+	+	-	+	-	-	-	-	-	-
9.	Охорона персональних даних	НД-09	-	+	+	-	+	-	-	-	+	+	+	+	-	-	-	-	-	+
10.	Організація та управління службою захисту інформації	НД-10	+	+	+	+	+	-	-	+	+	+	+	+	+	+	+	+	+	+
11.	Конкурентна розвідка	НД-11	-	+	-	+	+	+	+	+	-	+	+	+	+	-	+	-	-	+
12.	Комплексні системи захисту інформації	НД-12	+	+	+	-	-	-	-	-	-	+	-	-	-	-	-	-	-	-
13.	Правові засади охорони банківської таємниці	НД-13	+	+	+	-	+	+	+	+	+	+	+	+	-	+	+	-	-	-
14.	Міжнародні стандарти захисту інформації	НД-14	+	-	-	-	-	-	-	-	+	-	-	-	-	-	-	+	+	+
15.	Охорона комерційної таємниці	НД-15	+	+	+	+	+	+	+	+	+	+	+	+	+	-	-	-	-	+

Примітка: відповідність позначається символом «+», в іншому випадку символом «-».

III. Послідовність вивчення навчальних дисциплін:

Блоки дисциплін		1 семестр	2 семестр	3 семестр
Нормативна (обов'язкова) складова (33 кред.)	Цикл загальної підготовки	НД-03 Іноземна мова (професійного спрямування), 6 кредитів		
		НД-01 Методологія наукових досліджень, 3 кредити		
		НД-02 Теорія прийняття рішень, 4 кредити		
	Цикл професійної підготовки		НД-04 Менеджмент організацій, 4 кредити	НД-06 Кадрова політика в сфері захисту інформації з обмеженим доступом, 3 кредити
		НД-05 Антикризовий менеджмент, 4 кредити	НД-07 Науково-дослідна практика, 9 кредитів	
Вибіркова складова (57 кред.)	Цикл професійної підготовки (дисципліни спеціалізації)	Спеціалізація «Організація захисту інформації з обмеженим доступом»		
		НД-08 Охорона державної таємниці, 4 кредити	НД-44 Міжнародні стандарти захисту інформації, 4 кредити	НД-15 Охорона комерційної таємниці, 4 кредити
		НД-09 Охорона персональних даних, 3 кредити	НД-12 Комплексні системи захисту інформації, 5 кредитів	
		НД-10 Організація та управління службою захисту інформації, 4 кредити	НД-13 Правові засади охорони банківської таємниці, 4 кредити	
	НД-11 Конкурентна розвідка, 5 кредитів			
Вільний вибір здобувачів вищої освіти (дисципліни з переліку)		12 кредитів	12 кредитів	

ФОРМИ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

<p>Форми атестації здобувачів вищої освіти</p>	<p>Атестація здійснюватися у формі: 1) публічного захисту кваліфікаційної роботи; 2) публічного захисту кваліфікаційної роботи або комплексного екзамену (лише в 2020 р).</p>
<p>Вимоги до написання та захисту кваліфікаційної роботи кваліфікаційних робіт (за наявності)</p>	<p>Кваліфікаційна робота має передбачити розв'язання складної задачі або проблеми в сфері менеджменту, задачі або проблеми в сфері менеджменту, що потребує здійснення досліджень та /або інновацій і характеризується комплексністю і невизначеністю умов, із застосуванням теорії та методів сучасної науки.</p> <p>Кваліфікаційна робота не повинна містити академічного плагіату, фальсифікації, фабрикації. Робота має бути оприлюднена на офіційному сайті закладу вищої освіти або його підрозділу, або у репозитарії закладу вищої освіти</p>
<p>Вимоги до комплексного екзамену (за наявності)</p>	<p>Організація і проведення атестації здобувачів освіти здійснюється Національною академією СБ України у порядку, встановленому законодавством України та Положенням про екзаменаційну комісію Національної академії Служби безпеки України, затвердженим наказом НА СБУ від 16.01.2016 № 20 (зі змінами) (далі – Положення 20-2016).</p> <p>Екзамен (комплексний екзамен) проводиться відповідно до затвердженої програми, форма якої визначена додатком 1 до Положення 20-2016.</p> <p>Програма комплексного екзамену містить у собі найбільш вагомі, узагальнені питання декількох програм навчальних дисциплін професійної підготовки відповідної спеціальності.</p> <p>Програма екзамену (комплексного екзамену) розробляється відповідною кафедрою окремо з кожної спеціальності підготовки фахівців.</p> <p>Програма екзамену (комплексного екзамену) включає:</p> <ul style="list-style-type: none"> – цільову настанову та зміст програми, що розкривають питання програм навчальних дисциплін професійної підготовки за відповідною спеціальністю (спеціалізацією); – форму проведення (усна, письмова, поетапна тощо); – єдині вимоги до критеріїв та порядку оцінювання рівня сформованості знань та умінь здобувачів вищої освіти відповідно до компетентностей, що визначені в стандартах вищої освіти; – перелік нормативно-правових актів, навчальної основної та додаткової літератури. <p>Екзамен (комплексний екзамен) приймається за білетами, кожний з яких містить теоретичні питання, що стосуються різних розділів курсу і залежать від специфіки навчальної дисципліни. Для виявлення рівня практичної підготовки за фахом білетом може бути передбачено вирішення практичного завдання чи задачі. Кількість питань в білеті визначається програмою екзамену (комплексного екзамену) (додаток 2 до Положення 20-2016).</p> <p>Зміст екзаменаційних білетів повинен відповідати програмам навчальних дисциплін, з яких проводяться екзамен, а для комплексного екзамену – програмі комплексного екзамену.</p>

--	--

ВИМОГИ ДО НАЯВНОСТІ СИСТЕМИ ВНУТРІШНЬОГО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ ЗА ОСВІТНЬОЮ ПРОГРАМОЮ

У Національній академії СБ України функціонує система забезпечення якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості), яка передбачає здійснення таких процедур і заходів:

- визначення принципів та процедур забезпечення якості вищої освіти;
- здійснення щорічного моніторингу відповідності кадрового, навчально-методичного, інформаційного та матеріально-технічного забезпечення Ліцензійним умовам провадження освітньої діяльності закладів освіти та вироблення на його основі заходів, спрямованих на покращання відповідних складових освітньої діяльності;
- забезпечення аналізу виконання здобувачами освіти навчального (робочих навчальних) планів освітньої програми, контролю за якістю викладання навчальних дисциплін у порядку та строки, визначені розпорядчими документами Національної академії СБ України;
- здійснення моніторингу та періодичного перегляду освітньої програми;
- щорічне оцінювання здобувачів освіти, науково-педагогічних співробітників (працівників) Національної академії СБ України та регулярне оприлюднення результатів таких оцінювань на інформаційних стендах та/або в будь-який інший спосіб;
- забезпечення підвищення кваліфікації науково-педагогічних співробітників (працівників) Національної академії СБ України;
- забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи здобувачів освіти, за освітньою програмою;
- забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;
- забезпечення публічності інформації про освітню програму, ступінь вищої освіти та кваліфікації (освітню, професійну, у документі про освіту);
- забезпечення ефективної системи запобігання та виявлення академічного плагіату у наукових працях співробітників (працівників) Національної академії СБ України і здобувачів освіти;
- здійснення інших процедур і заходів.

Система забезпечення вищим навчальним закладом 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.

ПЕРЕЛІК НОРМАТИВНИХ, РОЗПОРЯДЧИХ, ІНСТРУКТИВНИХ ДОКУМЕНТІВ, НА ЯКИХ БАЗУЄТЬСЯ ОСВІТНЯ ПРОГРАМА

1. ESG – <http://ihed.org.ua/images/pdf/standards-and-guidelines-for-qa-in-the-eha-2015.pdf>
2. ISCED (МСКО) 2011 – <http://www.uis.unesco.org/education/documents/isced-2011-en.pdf>.
3. ISCED-F (МСКО-Г) 2013 – <http://www.uis.unesco.org/Education/Documents/isced-fields-of-education-training-2013.pdf>.
4. Закон «Про вищу освіту» - <http://zakon4.rada.gov.ua/laws/show/1556-18>.
5. Національний класифікатор України: «Класифікатор професій» ДК 003:2010.– К. : Видавництво «Соцінформ», 2010.
6. Національна рамка кваліфікацій – <http://zakon4.rada.gov.ua/laws/show/1341-2011-п>.
7. Перелік галузей знань і спеціальностей – <http://zakon4.rada.gov.ua/laws/show/266-2015-п>.
8. TUNING (для ознайомлення зі спеціальними (фаховими) компетентностями та прикладами стандартів – <http://www.unideusto.org/tuningeu/>.
9. Національний глосарій 2014 – http://ihed.org.ua/images/biblioteka/glossariy_Visha_osvita_2014_tempus-office.pdf.
10. Рашкевич Ю.М. Болонський процес та нова парадигма вищої освіти – <file:///D:/Users/Dell/Downloads/BolonskyiProcessNewParadigmHE.pdf>.
11. Розвиток системи забезпечення якості вищої освіти в Україні: інформаційно-аналітичний огляд – http://ihed.org.ua/images/biblioteka/Rozvitok_sisitemi_zabesp_yakosti_VO_UA_2015.pdf.
12. Розроблення освітніх програм: методичні рекомендації – http://ihed.org.ua/images/biblioteka/rozroblennya_osv_program_2014_tempus-office.pdf.
 - Закон України від 01.07.2014 № 1556-VII «Про вищу освіту». (із змінами) Закон України “Про національну безпеку України”.
 - Постанова Кабінету Міністрів України від 23.11.2011 № 1341(із змінами) “Про затвердження Національної рамки кваліфікацій”.
 - Національний класифікатор України “Класифікатор професій”, затверджений наказом Держспоживстандарту України від 28.07.2010 № 237 (із змінами).
 - Наказ Міністерства освіти і науки України від 01.06.2016 № 600 “Про затвердження та введення в дію Методичних рекомендацій щодо розроблення стандартів вищої освіти”(із змінами)
 - Стандарти і рекомендації щодо забезпечення якості в Європейському просторі вищої освіти (ESG). – К.: ТОВ “ІЦС”, 2015. – 32 с.
 - International Standard Classification of Education ISCED 2011. – UNESCO Institute for Statistics, 2012. – 84 p.
 - ISCED Fields of Education and Training 2013 (ISCED-F 2013): Manual to accompany the International Standard Classification of Education 2011. – UNESCO Institute for Statistics P.O., 2014. – 20 p.
 - Стандарт вищої освіти України за спеціальністю 073»Менеджмент», 10.07.2019 №959.
 - Положення про організацію освітнього процесу в Національній академії Служби безпеки України, затверджено наказом НА СБУ від 31.08.2015 № 234 (зі змінами).
 - Методичні рекомендації для розроблення профілів ступеневих програм, включаючи програмні компетентності та програмні результати навчання/ пер. З англ. Національного експерта з реформування вищої освіти Програми Еразмус+, д-ра техн. наук, проф. Ю.М.Рашкевича.– Київ: ТОВ «Поліграф плюс», 2016. – 80 с.

