

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

ЗАТВЕРДЖЕНО

Рішенням Вченої ради Національної академії
СБ України від 28 лютого 2019 р., протокол № 4

Ректор Національної академії СБ України
06.03.2019

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

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

| | |
|------------------|---|
| за спеціальністю | 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) |
| спеціалізацією | 256.04 Національна безпека (забезпечення державної безпеки в інформаційній сфері) |
| галузі знань | 25 Воєнні науки, національна безпека, безпека державного кордону |
| кваліфікація | магістр національної безпеки (забезпечення державної безпеки в інформаційній сфері); професіонал із організації захисту інформації з обмеженим доступом |

ПЕРЕДМОВА

Введено вперше, як тимчасовий документ до введення в дію стандарту вищої освіти України за відповідним рівнем вищої освіти за спеціальністю 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) спеціалізацією 256.04 Національна безпека (забезпечення державної безпеки в інформаційній сфері).

Розробники – проектна група, створена відповідно до Розпорядження НА СБ України від 23 січня 2019 року № 14 «Щодо створення тимчасової робочої групи з розробки освітньо-професійної програми «Організація захисту інформації з обмеженим доступом» та навчального плану підготовки здобувачів вищої освіти другого (магістерського) рівня за спеціальністю 256.04 Національна безпека (забезпечення державної безпеки в інформаційній сфері)» у складі:

Чеховська Марія Миколаївна, завідувач кафедри національної безпеки, доктор економічних наук, професор – керівник робочої групи;

Князев Сергій Олександрович, професор кафедри організації захисту інформації з обмеженим доступом Навчально-наукового інституту інформаційної безпеки, кандидат юридичних наук, старший науковий співробітник;

Ничитайло Ірина Михайлівна, доцент кафедри національної безпеки, кандидат юридичних наук доцент;

Ткачук Тарас Юрійович, заступник завідувача кафедри організації захисту інформації з обмеженим доступом Навчально-наукового інституту інформаційної безпеки, кандидат юридичних наук, доцент;

Гордієнко Сергій Борисович, професор кафедри Навчально-наукового інституту інформаційної безпеки, кандидат технічних наук, доцент.

Болдир Сергій Володимирович начальник Департаменту охорони державної таємниці та ліцензування СБ України;

Мельник Михайло Романович студент ННІ ІБ НА СБ України, заступник голови студентського парламенту.

I. Профіль освітньо-професійної програми «Організація захисту інформації з обмеженим доступом» другого (магістерського) рівня вищої освіти за спеціальністю 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) спеціалізацією 256.04 Національна безпека (забезпечення державної безпеки в інформаційній сфері)

| 1 – Загальна інформація | |
|---|--|
| Повна назва закладу вищої освіти | Національна академія Служби безпеки України, Київ |
| Ступінь вищої освіти та назва кваліфікації мовою оригіналу | Магістр національної безпеки (забезпечення державної безпеки в інформаційній сфері). Професіонал з організації захисту інформації з обмеженим доступом Присвоюється відповідно до вимог, що визначаються відповідним професійним стандартом (довідником кваліфікаційних характеристик) та в порядку атестації за результатами єдиного державного кваліфікаційного іспиту. |
| Офіційна назва освітньої програми | Організація захисту інформації з обмеженим доступом |
| Тип диплому та обсяг освітньої програми | Диплом магістра, одиничний ступінь, 90 кредитів ЄКТС, 1 рік 6 місяців |
| Акредитаційна інституція | Національна агенція забезпечення якості вищої освіти |
| Цикл / рівень | НРК України – 7 рівень, FQ-EHEA – другий цикл, QF-LLL – 7 рівень |
| Передумови | Наявність ступеня бакалавра, спеціаліста, магістра |
| Мова (и) викладання | Українська, англійська |
| Термін дії освітньої програми | 2 роки |
| Інтернет-адреса постійного розміщення опису освітньої програми | www.academy.ssu.gov.ua (відповідно до умов і порядку, що визначаються нормативно-правовими актами Служби безпеки України). |
| 2 – Мета освітньої програми | |
| Формування та розвиток спеціально-професійних компетентностей у галузі 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. | |
| 3 – Характеристика освітньої програми | |
| Предметна область (галузь знань, спеціальність, спеціалізація (і)) | 25 Воєнні науки, національна безпека, безпека державного кордону, 256 Національна безпека (за окремими сферами забезпечення і видами діяльності), 256.04 Національна безпека (забезпечення державної безпеки в інформаційній сфері). Об'єкт вивчення та діяльності – національні інтереси України в інформаційній сфері та загрози їх реалізації, заходи і засоби своєчасного |

| | |
|--|---|
| | виявлення, запобігання та нейтралізації загроз державній безпеці в інформаційній сфері. Теоретичним змістом предметної області є поняття, концепції, принципи, методи і методики, які використовуються для забезпечення інформаційної безпеки відповідно до компетенції Служби безпеки України, режимно-секретних органів України, інших заінтересованих суб'єктів національної безпеки України (за потреби). |
| Орієнтація освітньої програми | Програма пропонує комплексний підхід до управління сучасним підприємством та реалізує це через навчання та практичну підготовку. Програма професійна, прикладна, 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 сьогоденного стану та перспектив розвитку сфери захисту інформації з обмеженим доступом, орієнтує на подальшу професійну та наукову кар'єру. |
| Основний фокус освітньої програми та спеціалізації (й) | Організаційно-правові методи, засоби захисту інформації та система управління інформаційною безпекою. |
| Особливості програми | Програма розвиває перспективи професійної підготовки фахівців 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). |
| 4 – Придатність випусників до працевлаштування та подальшого навчання | |
| Придатність до працевлаштування | Професіонал підготовлений до діяльності в галузі економіки за кодами (назвами) ДК-009 2010: 62.09 (діяльність у сфері інформаційних технологій і комп'ютерних систем); 80.2 (обслуговування систем безпеки); 84.24 (діяльність у сфері охорони громадського порядку та безпеки) та здатний виконувати професійну роботу і може призначатися на посаду військовослужбовця Служби безпеки |

| | |
|-------------------------------------|--|
| | України відповідного профілю службової діяльності або займати первинні посади (за ДКП-003 2010): 2149.2 Професіонал із організації інформаційної безпеки; 2149.2 Професіонал із організації захисту інформації з обмеженим доступом. |
| Подальше навчання | Можливість навчання за програмою третього освітньо-наукового рівня вищої освіти за цією спеціальністю або за міждисциплінарними програмами. |
| 5 – Викладання та оцінювання | |
| Викладання та навчання | Студентоцентроване, проблемно-орієнтоване навчання, ініціативне самонавчання. Лекційні заняття мають інтерактивний 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. |
| Оцінювання | 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 роботи. 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. |
| 6 – Програмні компетентності | |
| Інтегральна компетентність | Здатність розв'язувати складні завдання і проблеми захисту інформації з обмеженим доступом, як важливої, специфічної складової інформаційної сфери |
| Загальні компетентності (ЗК) | <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 |

| | |
|----------------------------|--|
| | <p>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> <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.</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> |
| Фахові компетентності (ФК) | <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</p> |

| | |
|--|--|
| | <p>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 витoku 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> |
| 7 – Програмні результати навчання | |
| <p>Сукупність знань, умінь, навичок, інших компетентностей</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 умінь 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 організаційно-правового забезпечення охорони комерційної</p> |
|--|---|

| | |
|---|---|
| | таємниці. |
| Комунікація | Уміння спілкуватись науковою та професійною мовою, включаючи усну та письмову комунікацію державною мовою та принаймні однією із поширених європейських мов. Здатність використовувати різноманітні методи, зокрема сучасні інформаційні технології, для ефективної комунікації на професійному та соціальному рівнях. |
| Автономія і відповідальність | Здатність відповідально ставитись до виконання службової діяльності, самостійно приймати рішення, досягати поставленої мети з дотриманням вимог професійної етики. Здатність до самонавчання та продовження професійного розвитку. |
| 8 – Ресурсне забезпечення реалізації програми | |
| Основні характеристики кадрового забезпечення | До реалізації програми залучаються науково-педагогічні співробітники (працівники) з науковими ступенями та/або вченими званнями. Науково-педагогічні співробітники (працівники) один раз на п'ять років проходять стажування. |
| Основні характеристики матеріально-технічного забезпечення | Використання навчальних аудиторій, спеціальних кабінетів, укомплектованих технічними засобами навчання й контролю |
| Основні характеристики інформаційного та навчально-методичного забезпечення | Використання традиційних та електронних інформаційних ресурсів загальної бібліотеки, авторських розробок науково-педагогічних працівників Національної академії Служби безпеки України |
| 9 – Особливості освітньої програми | |
| Академічна мобільність | На загальних підставах в межах України |

II. 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 вищої освіти | 24/720 | | |
| 1.4. | Обсяг циклу загальної підготовки | 13/390 | | |
| 1.5. | Обсяг циклу професійної підготовки | 77/2310 | | |
| 2. Показники навчального навантаження здобувачів вищої 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 | 1,67 кр / 50 год. | | |
| 2.2.2. | мінімальне | 1,5 кр / 45 год. | | |
| 3. Показник співвідношення між навчальними заняттями і годинами самостійної роботи здобувачів вищої освіти (у кредитах ЄКТС/годинах) | | | | |
| 3.1. | Обсяг навчальних занять | 936 | | |
| 3.2. | Обсяг самостійної роботи | 1764 | | |
| 4. Загальні показники компонент освітньої програми | | | | |
| 4.1. | Мінімальний обсяг навчальної дисципліни (спецкурсу), (у кредитах ЄКТС/годинах) | 3/90 | | |
| 4.2. | Орієнтовна кількість навчальних дисциплін (спекурсів) / із них за вільним вибором здобувачів вищої освіти | 23/8 | | |
| 4.3. | Вид (и) практичної підготовки (тривалість у тижнях) | | | |
| 4.3.1. | Науково-дослідна практика | 9 | | |
| 4.4. | Форма та назва атестації (тривалість підготовки до неї в днях) | | | |
| 4.4.1. | Єдиний державний кваліфікаційний іспит | 5 днів | | |
| 5. Перелік компонент освітньої програми | | | | |
| Код н/д | Компоненти освітньої програми (навчальні дисципліни, спецкурси, курсові роботи, практики, кваліфікаційна робота) | Кількість кредитів ЄКТС | Форма підсумкового контролю | Номер додатка до освітньої програми |
| Обов'язкові компоненти освітньої програми | | | | |
| ОК-1 | Методологія наукових досліджень | 3 | диф. залік | додаток 1 |
| ОК-2 | Теорія прийняття рішень | 4 | диф. залік | додаток 2 |
| ОК-3 | Іноземна мова (професійного спрямування) | 6 | екзамен | додаток 3 |
| ОК-4 | Актуальні питання національної безпеки України | 3 | диф. залік | додаток 4 |
| ОК-5 | Теорія ризиків | 5 | екзамен | додаток 5 |
| ОК-6 | Кадрова політика в сфері захисту інформації з обмеженим доступом | 3 | диф. залік | додаток 6 |
| ОК-7 | Науково-дослідна практика | 9 | диф. залік | додаток 7 |
| Загальний обсяг обов'язкових компонент: | | 33 | | |

| Вибіркові компоненти освітньої програми | | | | |
|--|--|----|------------|------------|
| ВБ-1.1 | Охорона державної таємниці | 4 | екзамен | додаток 8 |
| ВБ-1.2 | Охорона персональних даних | 3 | диф. залік | додаток 9 |
| ВБ-1.3 | Організація та управління службою захисту інформації | 4 | екзамен | додаток 10 |
| ВБ-1.4 | Конкурентна розвідка | 5 | екзамен | додаток 11 |
| ВБ-1.5 | Комплексні системи захисту інформації | 5 | екзамен | додаток 12 |
| ВБ-1.6 | Правові засади охорони банківської таємниці | 4 | екзамен | додаток 13 |
| ВБ-1.7 | Міжнародні стандарти захисту інформації | 4 | диф. залік | додаток 14 |
| ВБ-1.8 | Охорона комерційної таємниці | 4 | диф. залік | додаток 15 |
| Дисципліни вільного вибору | | 24 | | |
| Загальний обсяг вибіркового компоненту: | | 57 | | |

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

3.1. 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 – ЗК) | | | | | | |
| № з/п | Шифр | Зміст | | | | |
| 1.1 | ЗК-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 державних 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 | ЗК-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 | ЗК-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 | ЗК-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 | ЗК-05 | <i>Здатність до навчання та готовність підвищувати рівень своїх знань.</i> Знання дієвих | 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 політики в залежності від виду | 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. |

| | | | | | | |
|-----|-------|--|--|--|--|---|
| | | 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. | | управління та характеру ситуації конкретного суб'єкту господарювання із 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. | Володіти основними нормами та правилами ділового етикету в менеджменті державних підприємств, установ і організацій. | 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. |
| 1.6 | ЗК-06 | <i>Знання ділової іноземної мови.</i> Вільне володіння, читання, аудіювання, письмо іноземною мовою. | Функціональної лексики англійської мови з тематики, що вивчається, для її подальшого вживання в усному та письмовому мовленні та при перекладі текстів за фахом; іншомовних особливості 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 | ЗК-07 | <i>Здатність до наукової діяльності.</i> 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. Сутності сучасних наукових концепцій менеджменту державних підприємств, установ і організацій. | 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 витоку інформації з обмеженим доступом, економічні, правові, соціальні, інженерно-технічні та побутові аспекти проблеми. Застосовувати принципи менеджменту державних підприємств, установ і організацій. | 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. Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування. |

| 2. Спеціальні (фахові) програмні компетентності (далі – ФК) | | | | | | |
|---|-------|--|---|---|---|---|
| 2.1 | ФК-01 | <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>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>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>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>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 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>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 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</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>Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування.</p> |

| | | | | | | |
|-----|-------|--|--|---|---|--|
| | | | 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 | ФК-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 рішення широкого кола загальних проблем і задач (завдань) з організації та захисту інформації з обмеженим доступом на підприємстві в установі, організації. | Знання з організації та розроблення комплексної системи захисту інформації з обмеженим доступом та формування системи суб'єктів захисту інформації з обмеженим доступом установ, підприємств, організації. | 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 системи безпеки на предмет відповідності міжнародним стандартам (ISO/IEC). | 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>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 знань у сфері охорони персональних даних.</p> |

| | | | | | | |
|-----|-------|--|--|---|---|--|
| 2.3 | ФК-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. | 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. | 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. |
| | | | Принципів моніторингу, протидії загрозам конфіденційності, цілісності, доступності інформації з обмеженим доступом і уміння їх використовувати. | 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. | Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування |
| 2.4 | ФК-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. | 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. | 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 |
| | | | 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. | 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. | 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. |
| | | | Організаційно-правових основ роботи конкурентної розвідки на підприємстві. | Визначати і характеризувати методологію інформаційно-аналітичної діяльності конкурентної розвідки; застосовувати інформаційно-аналітичні технології, які використовує в роботі конкурентної розвідки; створювати нові інформаційні продукти на основі аналітико-синтетичного опрацювання інформаційних матеріалів; | 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. |

| | | | | | | |
|-----|-------|--|---|---|---|--|
| | | | | використовувати методи конкурентної розвідки для збирання інформації з відкритих джерел; формувати конкурентну стратегію інформаційної безпеки підприємства; застосовувати способи використання наявних та перспективних інформаційних технологій для подальшого прогнозування результатів їх впровадження та вироблення управлінських рішень. | | |
| 2.5 | ФК-05 | <i>Професійна ерудиція.</i> Здатність навчати співробітників новим методам організації захисту інформації з обмеженим доступом. | Системи (органів, підрозділів), що забезпечує захист інформації з обмеженим доступом підприємств, установ організацій. | 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. | 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. | Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування. |
| | | | 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). | 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. | 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. | Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування. |
| | | | Основних положення трудового законодавства, вимог з питань охорони праці та техніки безпеки, пожежної безпеки, внутрішньооб'єктового та перепускного режиму, трудовий розпорядок, правила та засоби проведення профілактичної роботи. | 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); вести діяльність з дотриманням вимог трудового та інформаційного законодавства. | 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. | Прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування. |

3.2. Перелік результатів навчання та їх відповідність програмним компетентностям:

| Шифри програмних компетентностей | | ЗК-01 | ЗК-02 | ЗК-03 | ЗК-04 | ЗК-05 | ЗК-06 | ЗК-07 | ФК-01 | ФК-02 | ФК-03 | ФК-04 | ФК-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. | + | + | - | + | + | - | + | + | + | - | + | - |

Керівник проектної групи

М.Чеховська

| | | | | | | | | | | | | | |
|-------|--|---|---|---|---|---|---|---|---|---|---|---|---|
| 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. | + | + | - | - | + | - | - | + | + | + | + | - |

Керівник проектної групи

М.Чеховська

| | | | | | | | | | | | | | |
|-------|--|---|---|---|---|---|---|---|---|---|---|---|---|
| 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. | + | + | - | + | + | + | + | + | - | + | + | - |

IV. Логічна послідовність вивчення освітніх компонентів (навчальних дисциплін, спецкурсів):

| Блоки навчальних дисциплін | 1 курс | | 2 курс |
|--|--|--|---|
| | 1 семестр | 2 семестр | 3 семестр |
| | Обов'язкові дисципліни (33 кредити) | Методологія наукових досліджень, 3 кредити | |
| Теорія прийняття рішень, 4 кредити | | | |
| Іноземна мова (професійного спрямування), 6 кредитів | | | |
| | | Актуальні питання національної безпеки України, 3 кредити | |
| Цикл загальної підготовки | | Теорія ризиків, 5 кредити | |
| | | | Кадрова політика в сфері захисту інформації з обмеженим доступом, 3 кредити |
| | | | Науково-дослідна практика, 9 кредитів |
| | | | |
| Цикл професійної підготовки | Охорона державної таємниці, 4 кредити | | |
| | Охорона персональних даних, 3 кредити | | |
| | Організація та управління службою захисту інформації, 4 кредити | | |
| | Конкурентна розвідка, 5 кредитів | | |
| | | Комплексні системи захисту інформації, 5 кредитів | |
| | | Правові засади охорони банківської таємниці, 4 кредити | |
| | | Міжнародні стандарти захисту інформації, 4 кредити | |
| | | | Охорона комерційної таємниці, 4 кредити |
| Дисципліни вільного вибору | | | до 8 дисциплін, 24 кредити |

V. Форми атестації здобувачів вищої освіти

| | |
|---|---|
| Форми атестації здобувачів вищої освіти | Атестація – це встановлення відповідності засвоєних здобувачами освіти рівня та обсягу знань, умінь, інших компетентностей вимогам освітньої програми. Атестація випускників спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) спеціалізації 256.04 Національна безпека (забезпечення державної безпеки в інформаційній сфері) здійснюється у формі єдиного державного кваліфікаційного іспиту. Здобувачі вищої освіти можуть обирати магістерську роботу в межах вільного вибору як додаткову форму атестації. |
| Вимоги до написання кваліфікаційних робіт <i>(за наявності)</i> | Визначаються Положенням про кваліфікаційні роботи здобувачів вищої освіти в Національній академії СБ України від 01.11.2016 № 313 |
| Вимоги до захисту кваліфікаційних робіт <i>(за наявності)</i> | |
| Вимоги до екзамену <i>(за наявності)</i> | Організація і проведення атестації здобувачів освіти здійснюється Національною академією СБ України у порядку, встановленому законодавством та нормативно-правовими актами у сфері освітньої діяльності України та Положенням про екзаменаційну комісію Національної академії Служби безпеки України, затвердженим наказом НА СБУ від 16.01.2016 № 20 (зі змінами). |

VI. Система забезпечення якості освітньої діяльності та якості вищої освіти за освітньою програмою передбачає:

- 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 (індивідуальних 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 з урахуванням вимог нормативно-правових актів СБ України, 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.

VII. Вимоги професійних стандартів *(за наявності)*

VIII. Перелік нормативних документів, на яких базується освітня програма:

- Закон України від 01.07.2014 № 1556-VII «Про вищу освіту»;

- Постанова Кабінету Міністрів України від 23.11.2011 № 1341 «Про затвердження Національної рамки кваліфікацій»;

- Постанова Кабінету Міністрів України від 29.04.2015 № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти»;

- Постанова Кабінету Міністрів України від 01.02.2017 № 53 «Про внесення змін до Постанови Кабінету Міністрів України від 29.04.2015 № 266»;

- Національний класифікатор України «Класифікація видів економічної діяльності» ДК 009: 2010;

– Національний класифікатор України «Класифікатор професій», затверджений наказом Держспоживстандарту України від 28.07.2010 № 237 (із змінами);

– Наказ Центрального управління Служби безпеки України від 04.07.2017 № 410 «Про затвердження виду діяльності (спеціалізації) спеціальності 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)»;

– Наказ Міністерства освіти і науки України від 01.06.2016 № 600 «Про затвердження та введення в дію Методичних рекомендацій щодо розроблення стандартів вищої освіти»;

– Лист Міністерства освіти і науки України від 28.04.2017 № 1/9-239 щодо примірного зразка освітньо-професійної програми для першого (бакалаврського) та другого (магістерського) рівнів вищої освіти);

– Лист Міністерства освіти і науки України від 05.06.2018 № 1/9-377 щодо надання роз'яснень стосовно освітніх програм;

– Положення про організацію освітнього процесу в Національній академії Служби безпеки України, затверджено наказом НА СБУ від 31.08.2015 № 234 (зі змінами);

– Європейська кредитна трансферно-накопичувальна система: довідник користувача / пер. з англ.; за ред. д.т.н., проф. Ю.М. Рашкевича та д. пед.н., доц. Ж.В. Таланової. – Львів: Видавництво Львівської політехніки, 2015. – 106 с.;

– 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.;

– Національний освітній глосарій: вища освіта 2014;

– Проект Європейської Комісії «Гармонізація освітніх структур в Європі» (Tuning Educational Structures in Europe, TUNING);

– TUNING (для ознайомлення зі спеціальними (фаховими) компетентностями та прикладами стандартів);

– Рашкевич Ю.М. Болонський процес та нова парадигма вищої освіти;

– Розвиток системи забезпечення якості вищої освіти в Україні: інформаційно-аналітичний огляд, 2015;

– Стандарти і рекомендації щодо забезпечення якості в Європейському просторі вищої освіти (ESG), 2015.

Керівник проектної групи –
завідувач кафедри національної безпеки
Національної академії СБ України
М. Чеховська