МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ОСВІТНЯ ПРОГРАМА

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

першого (бакалаврського) рівня вищої освіти
(оновлена)

Спеціальність	**125 Кібербезпека та захист інформації**
Галузь знань	**12 Інформаційні технології**
Кваліфікація:	**Бакалавр з кібербезпеки та захисту інформації за освітньою програмою Управління інформаційною та кібернетичною безпекою**

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
Протокол № 10 від 01 квітня 2024 р.
Наказ № 64 від 01 квітня 2024 р.

Ректор _____ Володимир ТОЛУБКО

Освітня програма вводиться в дію з 01 вересня 2024 р.

Київ 2024

ЛИСТ ПОГОДЖЕННЯ

ОСВІТНЬОЇ ПРОГРАМИ
ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

галузь знань	12 «Інформаційні технології»
спеціальність	125 «Кібербезпека та захист інформації»
рівень вищої освіти	перший (бакалаврський)
кваліфікація	Бакалавр з кібербезпеки та захисту інформації за освітньою програмою Управління інформаційною та кібернетичною безпекою

1. Проректор з навчально-виховної роботи Вадим ВЛАСЕНКО
2. Проректор з навчально-виховної та наукової роботи Любов БЕРКМАН
3. Директор Навчально-методичного центру Ірина СРІБНА
4. Вчена рада Навчально-наукового інституту захисту інформації

Протокол № 8 від «01» квітня 2024 р.

Голова Вченої Ради ННІЗІ _____ Віталій САВЧЕНКО

5. Кафедра управління інформаційною та кібернетичною безпекою

Протокол № 10 від «01» квітня 2024 р.

Завідувач кафедри управління інформаційною та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА

Рецензії від зовнішніх стейкхолдерів (фірм-партнерів):

1. Товариство з обмеженою відповідальністю «ІТ спеціаліст»;
2. ДТ «ЕС ЕНД ТІ Україна»

ВІДОМОСТІ ПРО ПЕРЕГЛЯД ОСВІТНЬОЇ ПРОГРАМИ

Освітня програма переглянута та оновлена у зв'язку зі зміною назви Університету та у відповідності до:

Закону України «Про електронні комунікації» від 16.12.2020 № 1089-IX;

Постанови Кабінету Міністрів України «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 16.12.2022 № 1392;

Державного стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти (Наказ МОН України від 04.10.2018 № 1074);

Професійного стандарту на групу професій «Викладачі закладів вищої освіти» (Наказ Міністерства економіки від 23.03.2021 № 610);

Наказу Міністерства економіки України «Про затвердження зміни № 11 до національного класифікатора ДК 003:2010 «Класифікатор професій» від 29.12.2022 № 5573;

Наказу Міністерства економіки України «Про затвердження зміни № 13 до національного класифікатора ДК 003:2010» «Класифікатор професій» від 16.01.2024 № 1410;

рекомендацій акредитаційних комісій Університету; пропозицій роботодавців; побажань здобувачів вищої освіти.

1. Профіль освітньої програми

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Державний університет інформаційно-комунікаційних технологій, Навчально-науковий інститут захисту інформації
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	бакалавр освітня кваліфікація – бакалавр з кібербезпеки та захисту інформації за освітньою програмою Управління інформаційною та кібернетичною безпекою
Офіційна назва освітньої програми	Освітня програма «Управління інформаційною та кібернетичною безпекою»
Тип диплому та обсяг освітньої програми	диплом бакалавра, одиничний: на базі повної загальної середньої освіти - обсяг освітньої програми - 240 кредитів ЄКТС (термін навчання 3 роки та 10 місяців денної форми навчання та 4 роки 10 місяців заочної форми навчання); на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») заклад вищої освіти має право визнати та перезарахувати не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста); Прийом на основі ступенів «молодший бакалавр», здійснюється за результатами зовнішнього незалежного оцінювання в порядку, визначеному законодавством.
Наявність акредитації	Сертифікат про акредитацію спеціальності 125 Кібербезпека від УД №11008702 від 18.04.2019 Термін дії сертифікату до 01.07.2029 року.
Цикл/рівень	НРК України – 6 рівень/бакалавр, QF-EHEA- перший цикл, EQF-LLL – 6 рівень
Передумови	Наявність атестата про повну загальну середню освіту або диплому молодшого бакалавра (ОКР «молодший спеціаліст»)
Мова(и) викладання	Українська, англійська
Термін дії освітньої програми	Введена в дію з 01.09.2019 р. Програма дійсна впродовж терміну дії державних стандартів вищої освіти та може бути відкорегована відповідно до «Порядку розроблення, затвердження, моніторингу

	та внесення змін до освітніх програм та навчальних планів у Державному університеті інформаційно-комунікаційних технологій»
Інтернет - адреса постійного розміщення опису освітньої програми	https://www.dut.edu.ua/ua/1826-osvitno-profesiyni-programi-kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu

2 – Мета освітньої програми

Метою бакалаврської програми є підготовка бакалаврів із захисту інформації в інформаційних, комунікаційних та інформаційно-комунікаційних системах з правом подальшої професійної діяльності на державних та приватних підприємствах, організаціях, формування та розвиток у них загальних і професійних компетентностей у сфері інформаційної та/або кібернетичної безпеки, що забезпечують здатність випускника виконувати професійну діяльність на первинній посаді та впроваджувати технології інформаційної та/або кібербезпеки.

3 – Характеристика освітньої програми

Предметна область, напрям (галузь знань, спеціальність)	12 Інформаційні технології 125 Кібербезпека та захист інформації
Орієнтація освітньої програми	Освітня. 100 % обсягу освітньої програми спрямовано на забезпечення загальних і фахових компетенцій за спеціальністю 125 Кібербезпека та захист інформації, визначеного стандартом вищої освіти. Програма носить прикладний характер, спрямована на забезпечення потреб ринку праці, зокрема в галузі ІТ.
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта та професійна підготовка в галузі інформаційних технологій. Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки на підприємствах, в організаціях, установах. Ключові слова: РИЗИКИ, ЗАГРОЗИ І ВРАЗЛИВОСТІ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ, ЗАХИСТ ІНФОРМАЦІЇ, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРБЕЗПЕКОЮ.
Опис предметної області	Програма передбачає викладання навчальних компонент спеціалістами у сфері інформаційної та кібербезпеки та його інформаційно-аналітичного забезпечення, що суттєво поглиблює фахові компетентності майбутніх випускників. Передбачено проведення лекційних курсів, семінарських та практичних занять, лабораторних робіт з залученням фахівців з інформаційної та кібербезпеки. **Об'єкти професійної діяльності випускників**:

	об'єкти інформатизації, включаючи інформаційні, комунікаційні, інформаційно-комунікаційні, автоматизовані, інформаційно-аналітичні системи, інформаційні ресурси і технології; технології забезпечення безпеки інформації; процеси управління інформаційною та кібербезпекою об'єктів, що підлягають захисту. **Цілі навчання** підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та кібербезпеки. **Теоретичний зміст предметної діяльності** **Знання:** законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; принципів супроводу систем і комплексів інформаційної та кібербезпеки; теорії, моделей та принципів управління доступом до інформаційних ресурсів; теорії систем управління інформаційною та кібербезпекою; методів та засобів виявлення, управління та ідентифікації ризиків; методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; методів та засобів технічного та криптографічного захисту інформації; сучасних інформаційно-комунікаційних технологій; сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; автоматизованих систем проєктування. **Методи, методики та технології:** Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та кібербезпеки. **Інструменти та обладнання:** системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та кібербезпеки; сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Особливості програми	Програма передбачає: - викладання компонент циклу професійної підготовки англійською мовою; - отримання в межах навчального процесу сертифікатів від провідних компаній в галузі ІТ; - залучення до проведення семінарських, практичних занять та лабораторних робіт фахівців-практиків з інформаційної та кібербезпеки;

	- забезпечення умов підготовки здобувачів вищої освіти у реальному середовищі майбутньої професійної діяльності для набуття відповідних компетенцій шляхом організації проведення практик (ознайомча, виробнича та переддипломна) у організаціях і компаніях-партнерах з можливістю подальшого працевлаштування.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Бакалавр кібербезпеки за спеціалізацією Управління інформаційною та кібернетичною безпекою (випускник) здатний виконувати професійні роботи за Державним класифікатором професій ДК 003: 2010: **Основна:** **2139.2** – Аудитор інформаційних технологій (з кібербезпеки); **2139.2** – Фахівець із кібердосліджень та розробок систем безпеки; **2139.2** – Фахівець з питань безпеки. **Допоміжна:** **2139.2** – Аналітик загроз.
Академічні права випускників	Можливість продовжити навчання за освітньо-професійною програмою другого (магістерського) освітнього рівня вищої освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання і викладання. Викладання проводиться державною мовою. Іноземною (англійською) мовою проводиться викладання окремих дисциплін, які формують професійні компетентності. Викладання спрямоване на засвоєння знань, умінь і навичок для подальшого застосування на практиці. Основними способами передачі змісту освітньої програми є проведення лекцій, практичних, лабораторних та індивідуальних занять, консультацій, розв'язання ситуаційних завдань, тестування, презентації, ознайомча, виробнича, переддипломна практики.
Оцінювання	Види контролю: вхідний, поточний, рубіжний (модульний, тематичний) та підсумковий контроль. Оцінювання сформованих компетентностей проводиться під час контрольних заходів, які передбачені цією освітньою програмою та зазначені у навчальному плані. Критерії оцінювання знань, умінь та навичок здобувачів вищої освіти розроблені відповідно до чинного законодавства й затверджені у «Положенні про

	організацію освітнього процесу у Державному університеті інформаційно-комунікаційних технологій». З метою отримання додаткових балів в межах дисциплін зараховуються здобуті студентами сертифікати відомих компаній за тематикою дисциплін.
6 - Програмні компетенції	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані завдання та практичні проблеми у галузі забезпечення інформаційної та кібербезпеки, що характеризується комплексністю й неповною визначеністю умов.
Загальні компетентності (ЗК)	**ЗК 1.** Здатність застосовувати знання у практичних ситуаціях. **ЗК 2.** Знання та розуміння предметної області та розуміння професії. **ЗК 3.** Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. **ЗК 4.** Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. **ЗК 5.** Здатність до пошуку, оброблення та аналізу інформації. **ЗК 6.** Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. **ЗК 7.** Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Фахові компетентності (КФ)	**КФ 1.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та кібербезпеки. **КФ 2.** Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та кібербезпеки. **КФ 3.** Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-комунікаційних

	(автоматизованих) системах. **КФ 4.** Здатність забезпечувати неперервність бізнесу відповідно до встановленої політики безпеки. **КФ 5.** Здатність забезпечувати захист інформації, що обробляється в інформаційно-комунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки. **КФ 6.** Здатність відновлювати штатне функціонування інформаційних, інформаційно-комунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. **КФ 7.** Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних і технічних засобів і методів, процедур, практичних прийомів тощо). **КФ 8.** Здатність здійснювати процедури управління інцидентами інформаційної та кібербезпеки, проводити розслідування, надавати їм оцінку. **КФ 9.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. **КФ 10.** Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. **КФ 11.** Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-комунікаційних (автоматизованих) систем. **КФ 12**. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам.
7 – Програмні результати навчання	
	РН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. **РН 2.** Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих завдань і практичних проблем у професійній діяльності, оцінювати їхню ефективність. **РН 3.** Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих завдань професійної діяльності.

	РН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих завдань і практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. **РН 5.** Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. **РН 6.** Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. **РН 7.** Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, тому числі міжнародних в галузі інформаційної та /або кібербезпеки. **РН 8.** Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та кібербезпеки. **РН 9.** Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та кібербезпеки. **РН 10.** Виконувати аналіз і декомпозицію інформаційно-комунікаційних систем. **РН 11.** Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. **РН 12.** Розробляти моделі загроз та порушника інформаційної та кібербезпеки. **РН 13.** Аналізувати проєкти інформаційно-комунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних. **РН 14.** Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-комунікаційних системах програмно-апаратними засобами та давати оцінку якості прийнятих рішень. **РН 15.** Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. **РН 16.** Реалізовувати комплексні системи захисту інформації в автоматизованій системі організації (підприємства) відповідно до вимог нормативно-правових документів. **РН 17.** Забезпечувати процеси захисту та функціонування інформаційно-комунікаційних (автоматизованих) систем на основі практик, навичок і знань щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур і моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для

	внутрішніх і віддалених компонент. **РН 18.** Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. **РН 19**. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-комунікаційних системах. **РН 20.** Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в ІКС. **РН 21.** Вирішувати завдання забезпечення та супроводу (в тому числі: огляд, тестування, підзвітність) системи управління доступом відповідно до встановленої політики безпеки в інформаційних та інформаційно-комунікаційних (автоматизованих) системах. **РН 22.** Вирішувати завдання управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної та кібербезпеки. **РН 23.** Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-комунікаційних (автоматизованих) системах. **РН 24.** Вирішувати завдання управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-комунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових). **РН 25.** Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-комунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту. **РН 26.** Впроваджувати заходи та забезпечувати реалізацію процесів запобігання несанкціонованому доступу і захисту інформаційних, інформаційно-комунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем. **РН 27**. Вирішувати завдання захисту потоків даних в інформаційних, інформаційно-комунікаційних (автоматизованих) системах. **РН 28**. Аналізувати і проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-комунікаційних

	(автоматизованих) системах відповідно до встановленої політики інформаційної та кібербезпеки. **РН 29.** Виконувати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-комунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів. **РН 30.** Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-комунікаційних систем. **РН 31.** Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-комунікаційних систем. **РН 32.** Вирішувати завдання управління процесами відновлення штатного функціонування інформаційно-комунікаційних систем з використанням процедур резервування відповідно до встановленої політики безпеки. **РН 33.** Вирішувати завдання забезпечення неперервності бізнес процесів організації. **РН 34.** Брати участь у розробці та впровадженні стратегії інформаційної та кібербезпеки відповідно до цілей і завдань організації. **РН 35.** Вирішувати завдання забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-комунікаційних (автоматизованих) системах відповідно до встановленої політики інформаційної та кібербезпеки. **РН 36.** Виявляти небезпечні сигнали технічних засобів. **РН 37.** Вимірювати параметри небезпечних сигналів для технічних каналів витоку інформації та визначати ефективність захисту від витоку інформації відповідно до вимог нормативних документів системи технічного захисту інформації. **РН 38.** Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-комунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. **РН 39.** Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. **РН 40.** Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів інформаційної

	та кібербезпеки на основі автоматизованих процедур. **РН 41.** Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та кібербезпеки. **РН 42.** Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної та кібербезпеки для розслідування інцидентів. **РН 43.** Вирішувати задачі забезпечення неперервності бізнес процесів організації на основі встановленої системи управління інформаційною та кібербезпекою згідно з вітчизняними й міжнародними вимогами і стандартами. **РН 44.** Застосовувати різні класи політик інформаційної та кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів. **РН 45.** Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-комунікаційних системах. **РН 46.** Вирішувати завдання захисту інформації, що обробляється в інформаційно-комунікаційних системах з використанням сучасних методів і засобів криптографічного захисту інформації. **РН 47.** Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-комунікаційних системах. **РН 48.** Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-комунікаційних системах. **РН 49.** Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів і класів (статистичних, сигнатурних, статистично-сигнатурних). **РН 50.** Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-комунікаційних системах. **РН 51.** Використовувати інструментарій для моніторингу процесів в інформаційно-комунікаційних системах. **РН 52.** Вирішувати завдання аналізу програмного коду на наявність можливих вразливостей.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Група забезпечення спеціальності 125 Кібербезпека та захист інформації сформована із числа науково-

	педагогічних працівників Навчально-наукового інституту захисту інформації Державного університету інформаційно-комунікаційних технологій. Кількісний та якісний склад групи відповідають Ліцензійним вимогам.
Матеріально-технічне забезпечення	Теоретичні заняття проводяться в сучасних комп'ютерних класах і спеціалізованих лабораторіях, які оснащені спеціалізованими апаратно-програмними засобами. Для проведення практичних і лабораторних занять з метою формування професійних компетентностей зі спеціальності 125 Кібербезпека та захист інформації використовуються спеціалізовані лабораторії університету, які оснащені сучасними комп'ютерами та програмно-апаратними комплексами. НАВЧАЛЬНА ЛАБОРАТОРІЯ АКАДЕМІЧНИЙ ЦЕНТР КОМПЕТЕНЦІЙ IBM «КІБЕРПОЛІГОН» Лабораторія призначена для проведення практичних занять з використанням програмно-апаратних комплексів: IBM QRadar SIEM, IBM i2 Analyze Notebook Premium, Tenable Nessus Professional. Лабораторія дозволяє відпрацьовувати навички роботи у Центрі забезпечення кібербезпеки (Security Operation Center) з використанням технологій моніторингу, виявлення, аналізу та реагування на кіберінциденти в корпоративних інформаційних системах. НАВЧАЛЬНА ЛАБОРАТОРІЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ НА БАЗІ ТЕХНОЛОГІЙ «АВТОР» Лабораторія використовується для вивчення спеціалізованих засобів криптографічного захисту на базі продуктів компанії АВТОР – партнера кафедри інформаційної та кібернетичної безпеки. Крім того, в лабораторії проводяться тренінги з використанням криптографічних засобів захисту інформації в інформаційно-комунікаційних системах, віртуальних приватних мереж VPN, електронного цифрового підпису та інфраструктури відкритих ключів. Лабораторія дозволяє вивчати й застосовувати програмно-технічний комплекс «Центр сертифікації ключів», засоби криптографічного захисту IP-шифратор CryptoIP-448, електронні ключі "SecureToken-337, програмний IP-шифратор «CryptoIP-VPN Client», безконтактні кард-рідери КР-382, USB. НАВЧАЛЬНА ЛАБОРАТОРІЯ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ CISCO

	Лабораторія призначена для вивчення технологій мережевої безпеки CISCO, проведення тренінгів з впровадження технології HoneyPot щодо протидії кібератакам зловмисників на корпоративні інформаційні системи та сертифікаційних курсів від партнера кафедри інформаційної та кібернетичної безпеки – компанії CISCO: Introduction to Cybersecurity, CCNA Security, CCNA Cybersecurity Operations. НАВЧАЛЬНА ЛАБОРАТОРІЯ «ЦЕНТР УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРБЕЗПЕКОЮ» (SECURITY OPERATION CENTER) Лабораторія призначена для проведення занять з питань аналізу, обробки та аудиту інформаційної та кібербезпеки за допомогою SIEM-систем і програмних сканерів типу Nessus та Kali Linux. Крім того, дозволяє вивчати методи управління ризиками на основі методологій CRAMM, OCTAVE та RiskWatch у відповідності до вимог міжнародних стандартів з інформаційної та кібербезпеки. Лабораторія дозволяє працювати з програмними засобами підтримки прийняття рішень у сфері інформаційної та кібербезпеки («Вибір», Mpriority 1.0). НАВЧАЛЬНА ЛАБОРАТОРІЯ ЗАСОБІВ КОНТРОЛЮ ДОСТУПУ «HIKVISION» Лабораторія забезпечує проведення практичних занять та досліджень з питань контролю й управління доступом, використання автономних біометричних терміналів, мережевих контролерів, програмно-апаратного комплексу системи відеоспостереження HikVision. Лабораторія обладнана автоматизованим комплексом відеоспостереження та охорони об'єктів інформаційної діяльності (Harbor), програмно-апаратними комплексами контролю доступу (HikVision), сповіщувачами інфрачервоними (SRP 600) та магніто-контактними (СОМК-10), дозволяє вивчати питання застосування програмних комплексів захисту інформації («Лоза», «Гриф», «Рубіж»). НАВЧАЛЬНА ЛАБОРАТОРІЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ «РІАС» Лабораторія забезпечує проведення практичних занять з питань технічного захисту конфіденційної інформації на об'єктах інформаційної діяльності від витоку акустичним, віброакустичним та електромагнітним каналами з використанням широкосмугових генераторів акустичного та електромагнітного шуму

	(Ріас-2ГС, ГШ 1000, «Беркут»). Крім того, у лабораторії досліджуються питання застосування пошукового програмно-апаратного комплексу DigiSkan EX, методів виявлення випромінювань за допомогою індикаторів поля типу PROTEKT; порядку застосування скануючих приймачів AR 8200, IC-R5, IC-R2500 та локатора нелінійностей NR-900 EM.
Інформаційне та навчально-методичне забезпечення	Усі компоненти навчального плану забезпечені інформаційними й навчально-методичними матеріалами та розміщені у системі дистанційного навчання Moodle.
9 – Академічна мобільність	
Національна кредитна мобільність	Наявність двосторонніх договорів між Державним університетом інформаційно-комунікаційних технологій та закладами вищої освіти України забезпечує національну кредитну мобільність.
Міжнародна кредитна мобільність	Зміст освітньої програми відповідає стандартам вищої освіти, що дозволяє здобувачам брати участь у програмах подвійних дипломів та бути конкурентоспроможним на світовому ринку праці.
Навчання іноземних здобувачів вищої освіти	Програма передбачає навчання іноземців та осіб без громадянства.

2. Перелік компонент освітньої програми та їх логічна послідовність

2.1. Зміст підготовки за освітньою програмою компетентності та результатами навчання

№ п.п.	Компонента	Шифр	Компетентність	Результат навчання
1. Цикл компонент загальної підготовки				
1.	Вища математика	ЗК1.13.1.01	ЗК 6, КФ4	ПРН 8
2.	Основи управління інформаційною та кібербезпекою	ЗК1.13.1.02	ЗК 2, ЗК 3, КФ2, КФ7	РН 7, РН 14
3.	Засади відкриття власного бізнесу	ЗК1.13.1.03	ЗК 4, ЗК 5, ЗК 7, КФ1	РН 4, РН 9, РН 16, РН 20
4.	Філософія	ЗК1.13.1.04	ЗК 1, ЗК 2, ЗК 5, ЗК 6, КФ2	РН 1
5.	Іноземна мова*	ЗК1.13.1.05	ЗК 1, КФ3	РН 2
6.	Українська мова за професійним спрямуванням	ЗК1.13.1.06	ЗК 1, ЗК 5, ЗК 7, КФ1	РН 1, РН 2, РН 4
7.	Групова динаміка і комунікації	ЗК1.13.1.07	ЗК 1, ЗК 5, ЗК 7, КФ1	РН 1, РН 2, РН 4
8.	Соціально-екологічна безпека життєдіяльності	ЗК1.13.1.08	ЗК 6, КФ1	РН 9
7.	Нормативно-правове забезпечення інформаційної безпеки	ЗК1.13.1.09	ЗК 7, КФ4	РН 4, РН 9, РН 16, РН 20
10.	Фізика	ЗК1.13.1.10	ЗК 1, ЗК 2, КФ1	РН 8
11.	Теорія інформації та кодування	ЗК1.13.1.11	ЗК 3, КФ1, КФ2, КФ6, КФ7	РН 3, РН 5
12.	Стандарти інформаційної та кібербезпеки	ЗК1.13.1.12	ЗК 3, КФ6, КФ7, КФ8	РН 4, РН 16, РН 17, РН 19
2. Цикл компонент професійної та практичної підготовки				
1.	Теорія кіл і сигналів в інформаційному та кіберпросторах	ПП1.13.2.01	ЗК 3, КФ1, КФ2, КФ6, КФ7	РН 3, РН 5, РН 36, РН 37, РН 38, РН 39
2.	Прикладне програмування	ПП1.13.2.02	ЗК 4, КФ5, КФ6	РН 8, РН 12
3.	Основи інформаційних технологій	ПП1.13.2.03	ЗК 3, КФ1, КФ4, КФ5, КФ7	РН 5, РН 7, РН 9, РН 10, РН 11
4.	Операційні системи	ПП1.13.2.04	ЗК 3, КФ1, КФ4, КФ5, КФ7	РН 5, РН 7, РН 10, РН 12

5.	Аналіз та оцінка уразливостей інформаційних систем	ПП1.13..2.05	ЗК1, ЗК4, ЗК5, КФ8, КФ11, КФ12	РН3, РН9, РН18, РН28, РН35, РН51
6.	Захист від шкідливого програмного засобу	ПП1.13.2.06	ЗК1, ЗК4, КФ5, КФ6, КФ9	РН5, РН14, РН18, РН20, РН49, РН50, РН51, РН52
7.	Прикладна криптологія	ПП1.13.2.07	ЗК 3, КФ6, КФ7, КФ8	РН 8, РН 17, РН 18
8.	Хмарні технології	ПП1.13.2.08	ЗК 3, КФ1, КФ4, КФ5, КФ11	РН 14
9.	Комплексні системи захисту інформації	ПП1.13.2.09	ЗК 3, ЗК 4, КФ5, КФ6, КФ7, КФ8	РН 3, РН 4, РН 5, РН 6, РН 7, РН 9, РН 13, РН 14, РН 16, РН 19 РН26, РН35, РН50
10.	Штучний інтелект	ПП1.13.2.10	ЗК 3, КФ1, КФ4, КФ5, КФ11	РН 10, РН 15, РН 16
11.	Основи національної безпеки	ПП1.13.2.11	ЗК2, ЗК4, КФ 5, КФ 6, КФ 11, КФ2	РН12, РН14, РН15, РН21, РН23, РН25, РН27,РН49, РН51, РН52
12.	Інформаційна безпека держави	ПП1.13.2.12	ЗК2, ЗК5, КФ 2	РН6, РН12, РН19, РН29, РН31, РН32, РН48
13.	Система менеджменту інформаційної безпеки	ПП1.13.2.13	ЗК2, КФ 2	РН33
14.	Теорія ризиків	ПП1.13.2.14	ЗК2, ЗК5, КФ 8	РН4, РН12, РН19, РН23
15.	Системний аналіз інформаційної безпеки	ПП1.13.2.15	ЗК1, ЗК5, КФ 1, КФ 10	РН1, РН7, РН46, РН47
16.	Цифрова криміналістика	ПП1.13.2.16	ЗК1, ЗК2, ЗК5, ЗК7, КФ 1, КФ 6, КФ 8, КФ 10, КФ 11, КФ 12	РН15, РН21, РН 23, РН24, РН28, РН34, РН41, РН42, РН45
17.	Економічна безпека діяльності підприємств	ПП1.13.2.17	ЗК2, ЗК5, КФ 1, КФ 4, КФ 5	РН4, РН19, РН22, 28, РН44
18.	SIEM системи	ПП1.13.2.18	ЗК2, ЗК3, ЗК4, КФ 2, КФ 4, КФ 5, КФ 8, КФ 9, КФ 11, КФ 12	РН11, РН15, РН18, РН21, РН22, РН23, РН24, РН25, РН27, РН28, РН29, РН 40, РН43, РН48, РН 47, РН 51
19.	Організаційне забезпечення захисту інформації	ПП1.13.2.19	ЗК1, ЗК3, ЗК4, КФ1, КФ4, КФ6,	РН5, РН8, РН15, РН22, РН23,

			КФ8, КФ9, КФ11, КФ12	РН24, РН27, РН26 РН30, РН43 РН50
20.	Організація конфіденційного діловодства	ПП1.13.2.20	ЗК2, КФ2	РН5, РН13
21.	Аудит систем менеджменту інформаційної безпеки	ПП1.13.2.21	ЗК1, ЗК5, КФ1, КФ9	РН6, РН 15, РН 22, РН28, РН 36, РН 37, РН 38, РН 39, РН 46, РН47
22.	Основи телекомунікацій	ПП1.13.2.22	ЗК2,ЗК5, КФ2, КФ11,	РН10,РН13,РН17, РН27, РН48
23.	Стратегічні комунікації	ПП1.13.2.23	ЗК1, ЗК4, КФ1	РН5, РН33
24.	Ознайомча практика	ПП1.13.2.24	ЗК1, ЗК4	РН2, РН3, РН7
25.	Виробнича практика	ПП1.13.2.25	ЗК1, ЗК4	РН2, РН3, РН7, РН26, РН35, РН50
26.	Переддипломна практика	ПП1.13.2.26	ЗК2, ЗК4, ЗК5	РН2,РН3,РН 4, РН7
27.	Підготовка кваліфікаційної роботи	ПП1.13.2.27	ЗК1, ЗК2, ЗК4, ЗК5, КФ1	РН2, РН3, РН 4, РН 6, РН7
3.Дисципліни вільного вибору студента				
1.	Компонента вільного вибору студента			
2.	Компонента вільного вибору студента			
3.	Компонента вільного вибору студента			
4.	Компонента вільного вибору студента			
5.	Компонента вільного вибору студента			
6.	Компонента вільного вибору студента			
7.	Компонента вільного вибору студента			
8.	Компонента вільного вибору студента			
9.	Компонента вільного вибору студента			
10.	Компонента вільного вибору студента			
11.	Компонента вільного вибору студента			
12.	Компонента вільного вибору студента			

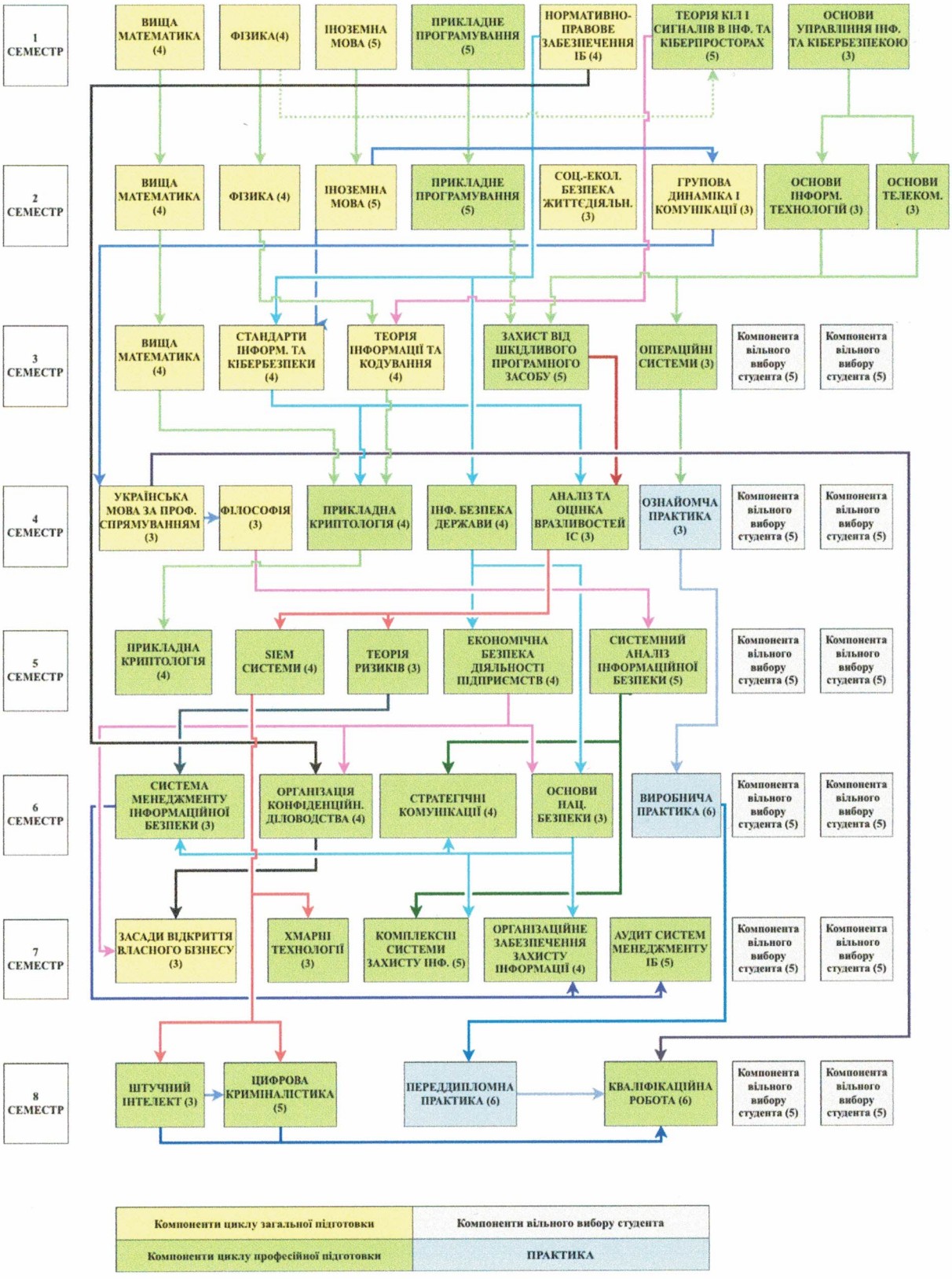
* Іноземна мова у навчальних планах для іноземців та осіб без громадянства замінюються на українську мову (за професійним спрямуванням).

2.2. Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
Обов'язкові компоненти ОП			
ЗК1.13.1.01	Вища математика	12	Залік, залік, Іспит
ЗК1.13.1.02	Основи інформаційної та кібербезпеки	3	Залік
ЗК1.13.1.03	Засади відкриття власного бізнесу	3	Залік
ЗК1.13.1.04	Філософія	3	Іспит
ЗК1.13.1.05	Іноземна мова	10	Залік, Іспит
ЗК1.13.1.06	Українська мова за професійним спрямуванням	3	Залік
ЗК1.13.1.07	Групова динаміка і комунікації	4	Залік
ЗК1.13.1.08	Соціально-екологічна безпека життєдіяльності	3	Іспит
ЗК1.13.1.09	Нормативно-правове забезпечення інформаційної безпеки	4	Іспит
ЗК1.13.1.10	Фізика	8	Залік, Іспит
ЗК1.13.1.11	Теорія інформації та кодування	4	Іспит
ЗК1.13.1.12	Стандарти інформаційної та кібербезпеки	3	Іспит
ПП1.13.2.01	Теорія кіл і сигналів в інформаційному та кіберпросторах	5	Іспит Курсова робота
ПП1.13.2.02	Прикладне програмування	10	Залік, Іспит Курсова робота
ПП1.13.2.03	Основи інформаційних технологій	5	Залік
ПП1.13.2.04	Операційні системи	3	Іспит
ПП1.13.2.05	Аналіз та оцінка уразливостей інформаційних систем	3	Іспит
ПП1.13.2.06	Захист від шкідливого програмного засобу	6	Залік
ПП1.13.2.07	Прикладна криптологія	8	Залік, Іспит Курсова робота
ПП1.13.2.08	Хмарні технології	3	Залік
ПП1.13.2.09	Комплексні системи захисту інформації	10	Іспит, Курсова робота
ПП1.13.2.10	Штучний інтелект	3	Іспит
ПП1.13.2.11	Основи національної безпеки	3	Іспит
ПП1.13.2.12	Інформаційна безпека держави	4	Іспит
ПП1.13.2.13	Система менеджменту інформаційної безпеки	3	Іспит
ПП1.13.2.14	Теорія ризиків	3	Залік
ПП1.13.2.15	Системний аналіз інформаційної безпеки	5	Залік
ПП1.13.2.16	Цифрова криміналістика	5	Іспит
ПП1.13.2.17	Економічна безпека діяльності підприємств	4	Залік
ПП1.13.2.18	SIEM системи	4	Іспит
ПП1.13.2.19	Організаційне забезпечення захисту інформації	4	Іспит

ПП1.13.2.20	Організація конфіденційного діловодства	3	Залік
ПП1.13.2.21	Аудит систем менеджменту інформаційних систем	3	Залік
ПП1.13.2.22	Основи телекомунікацій	2	Залік
ПП1.13.2.23	Стратегічні комунікації	6	Залік
ПП1.13.2.24	Ознайомча практика	3	Залік
ПП1.13.2.25	Виробнича практика	6	Залік
ПП1.13.2.26	Переддипломна практика	6	Залік
ПП1.13.2.27	Кваліфікаційна робота, атестація	6	Залік
Загальний обсяг обов'язкових компонент:		**180**	
Вибіркові компоненти ОП			
ВК1	Компонента вільного вибору студента	5	Залік
ВК2	Компонента вільного вибору студента	5	Залік
ВК3	Компонента вільного вибору студента	5	Залік
ВК4	Компонента вільного вибору студента	5	Залік
ВК5	Компонента вільного вибору студента	5	Залік
ВК6	Компонента вільного вибору студента	5	Залік
ВК7	Компонента вільного вибору студента	5	Залік
ВК8	Компонента вільного вибору студента	5	Залік
ВК9	Компонента вільного вибору студента	5	Залік
ВК10	Компонента вільного вибору студента	5	Залік
ВК11	Компонента вільного вибору студента	5	Залік
ВК12	Компонента вільного вибору студента	5	Залік
Загальний обсяг вибіркових компонент:		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

2.3. Структурно-логічна схема ОП



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здобувачів вищої освіти здійснюється у формі публічного захисту кваліфікаційної роботи або у формі єдиного державного кваліфікаційного іспиту (відповідно до стандарту 125 «Кібербезпека» зі змінами, внесеними на основі наказу Міністерства освіти і науки України від 13.01.2022 № 26).
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота передбачає розв'язання спеціалізованого завдання в галузі інформаційної та кібербезпеки. Робота має бути перевірена на плагіат відповідно до «Положення про запобігання академічному плагіату у Державному університеті інформаційно-комунікаційних технологій» та оприлюднена у депозитарію Університету. Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених цим стандартом та освітньою програмою (зміни внесені відповідно до наказу Міністерства освіти і науки України від 13.01.2022 № 26).

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ЗК1.13.1.01	ЗК1.13.1.02	ЗК1.13.1.03	ЗК1.13.1.04	ЗК 1.13.2.05	ЗК 1.13.2.06	ЗК 1.13.2.07	ЗК 1.13.2.08	ЗК 1.13.2.09	ЗК 1.13.2.10	ЗК 1.13.2.11	ЗК 1.13.2.12	ПП1.13.2.01	ПП1.13.2.02	ПП1.13.2.03	ПП1.13.2.04	ПП1.13.2.05	ПП1.13.2.06	ПП1.13.2.07	ПП1.13.2.08	ПП1.13.2.09	ПП1.13.2.10	ПП1.13.2.11	ПП1.13.2.12	ПП1.13.2.13	ПП1.13.2.14	ПП1.13.2.15	ПП1.13.2.16	ПП1.13.2.17	ПП1.13.2.18	ПП1.13.2.19	ПП1.13.2.20	ПП1.13.2.21	ПП1.13.2.22	ПП1.13.2.23	ПП1.13.2.24	ПП1.13.2.25	ПП1.13.2.26	ПП1.13.2.27
ЗК 1				•	•	•	•			•							•	•									•	•			•			•	•	•		•
ЗК 2		•		•						•													•	•	•	•		•	•	•	•		•				•	•
ЗК 3		•									•	•	•		•	•			•	•	•	•								•	•							
ЗК 4			•											•			•	•			•		•							•	•				•	•	•	•
ЗК 5			•	•		•	•										•							•		•	•	•	•				•		•			•
ЗК 6	•			•				•																														
ЗК 7			•																									•										
КФ 1			•			•	•	•		•	•		•		•	•				•		•					•	•	•		•			•				•
КФ 2		•		•							•		•											•	•					•		•	•					
КФ 3					•																																	
КФ 4	•								•						•	•				•		•							•	•	•							
КФ 5														•	•	•		•		•	•	•	•							•	•		•						
КФ 6											•	•	•	•				•	•		•		•						•			•						
КФ 7		•							•		•	•	•		•	•			•		•																	
КФ 8												•					•		•		•					•		•		•	•							
КФ 9																		•												•	•			•				
КФ10																											•	•										
КФ11																	•			•		•	•					•		•	•							
КФ12																	•						•					•		•	•							

5. Матриця забезпечення програмних результатів навчання (РН) відповідними компонентами освітньої програми

	ЗК1.13.1.01	ЗК1.13.1.02	ЗК1.13.1.03	ЗК1.13.1.04	ЗК 1.13.2.05	ЗК 1.13.2.06	ЗК 1.13.2.07	ЗК 1.13.2.08	ЗК 1.13.2.09	ЗК 1.13.2.10	ЗК 1.13.2.11	ЗК 1.13.2.12	ППІ1.13.2.01	ППІ1.13.2.02	ППІ1.13.2.03	ППІ1.13.2.04	ППІ1.13.2.05	ППІ1.13.2.06	ППІ1.13.2.07	ППІ1.13.2.08	ППІ1.13.2.09	ППІ1.13.2.10	ППІ1.13.2.11	ППІ1.13.2.12	ППІ1.13.2.13	ППІ1.13.2.14	ППІ1.13.2.15	ППІ1.13.2.16	ППІ1.13.2.17	ППІ1.13.2.18	ППІ1.13.2.19	ППІ1.13.2.20	ППІ1.13.2.21	ППІ1.13.2.22	ППІ1.13.2.23	ППІ1.13.2.24	ППІ1.13.2.25	ППІ1.13.2.26	ППІ1.13.2.27
РН 1				•		•	•																				•										
РН 2					•	•	•																												•	•	•	•
РН 3											•		•				•				•														•	•	•	•
РН 4			•			•	•		•			•									•					•			•						•		•
РН 5											•		•		•	•		•			•										•	•		•				
РН 6																					•			•								•						
РН 7		•													•	•					•						•								•	•	•	•
РН 8	•									•				•					•												•							
РН 9			•					•	•						•		•				•																	
РН 10															•	•						•											•					
РН 11															•															•								
РН 12														•		•							•	•		•												
РН 13																					•										•		•					
РН 14		•																•		•	•		•															
РН 15																						•	•					•		•	•		•					
РН 16			•						•			•									•	•																
РН 17												•							•														•					
РН 18																	•	•	•											•								
РН 19												•									•			•		•			•									
РН 20			•						•									•																				
РН 21																							•					•		•								
РН 22																													•	•	•		•					
РН 23																							•			•		•		•	•							
РН 24																												•		•	•							
РН 25																							•							•								
РН 26																					•										•					•		
РН 27																							•							•	•			•				
РН 28																	•											•	•	•			•					
РН 29																								•						•								
РН 30																															•							
РН 31																								•														
РН 32																								•														
РН 33																									•									•				
РН 34																												•										
РН 35																	•				•															•		
РН 36													•																				•					
РН 37													•																				•					
РН 38													•																				•					
РН 39													•																				•					
РН 40																														•								
РН 41																												•										
РН 42																												•										
РН 43																														•	•							
РН 44																													•									
РН 45																												•										
РН 46																											•					•						
РН 47																											•			•		•						
РН 48																								•						•								
РН 49																		•				•																
РН 50																		•		•											•					•		
РН 51																	•	•				•								•								
РН 52																		•				•																

Гарант освітньої програми
Доцент кафедри управління інформаційною
та кібернетичною безпекою
Навчально-наукового інституту захисту інформації
Державного університету
інформаційно-комунікаційних технологій
Кандидат наук з державного управління, доцент Тетяна МУЖАНОВА