

**ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА  
«КІБЕРБЕЗПЕКА»**

<b>РІВЕНЬ ВИЩОЇ ОСВІТИ</b>	<b>Перший (бакалаврський)</b>
<b>СТУПІНЬ ВИЩОЇ ОСВІТИ</b>	<b>Бакалавр</b>
<b>ГАЛУЗЬ ЗНАНЬ</b>	<b>12 Інформаційні технології</b>
<b>СПЕЦІАЛЬНІСТЬ</b>	<b>125 Кібербезпека</b>

## **ПРЕАМБУЛА**

Робоча група освітньої програми:

Лимаренко Вячеслав Володимирович, доцент кафедри кібербезпеки та інформаційних технологій, кандидат технічних наук – гарант освітньої-професійної програми.

Шаповалова Олена Олександрівна, доцент кафедри кібербезпеки та інформаційних технологій, кандидат технічних наук, доцент.

Венгріна Олена Сергіївна, доцент кафедри кібербезпеки та інформаційних технологій, кандидат технічних наук.

Пожидаєв Максим Геннадійович, здобувач вищої освіти.

Бондар Сергій Володимирович, менеджер ТОВ «Охорона і безпека».

ОП оновлено на підставі:

1. Законодавчих та нормативних актів: Законів України “Про освіту”, “Про вищу освіту”, Національної рамки кваліфікації, Національного класифікатору України.

2. Стандарту вищої освіти України: перший (бакалаврський) рівень, галузь знань 12 – Інформаційні технології, спеціальність 125 – Кібербезпека, затвердженого Наказом Міністерства освіти та науки України № 1074 від 04.10.2018 р.).

3. Аналізу ринку праці, з урахуванням регіонального контексту.

4. Вивчення вітчизняного та зарубіжного досвіду.

5. Пропозицій роботодавців.

6. Рекомендації після процедур акредитація Національного агентства із забезпечення якості вищої освіти рішення від 27.04.2021, протокол № 7.

Рецензії-відгуки зовнішніх стейкхолдерів (додаються).

**ПРОЕКТ освітньої програми для обговорення на 2023-2024 навчальний рік****I. ЗАГАЛЬНА ХАРАКТЕРИСТИКА**

<b>Рівень вищої освіти</b>	Перший (бакалаврський) рівень
<b>Ступінь вищої освіти</b>	Бакалавр
<b>Галузі знань</b>	12 Інформаційні технології
<b>Спеціальності</b>	125 Кібербезпека
<b>Освітня програма (укр. та англ. мовою)</b>	Кібербезпека / Cybersecurity
<b>Форми здобуття освіти, обсяг освітньої програми в кредитах ЄКТС та терміни навчання</b>	– на базі повної загальної середньої освіти: денна форма – 240 кредитів, 3 роки 10 місяців. – на базі ступеня “молодший бакалавр” (освітньо-кваліфікаційного рівня “молодший спеціаліст”): денна форма – 240 кредитів, 2 роки 10 місяців.
<b>Наявність акредитації</b>	Сертифікат про акредитацію освітньої програми НАЗЯВО № 1484 від 29.04.2021 строк дії сертифіката про акредитацію освітньої програми до 01.07.2026
<b>Мова(и) навчання / оцінювання</b>	українська / англійська
<b>Структурний підрозділ відповідальний за ОП</b>	Кафедра кібербезпеки та інформаційних технологій; Навчальна лабораторія кафедри кібербезпеки та інформаційних технологій
<b>Вимоги до зарахування</b>	Набір на перший (бакалаврський) рівень вищої освіти здійснюється за результатами складання національного мультипредметного тесту та мотиваційного листа. Для успішного засвоєння освітньої програми бакалавра абітурієнти повинні мати повну загальну середню освіту та прагнення оволодіти знаннями у галузі інформаційних технологій зі спеціальності кібербезпека. Правила та строки прийому розміщені на сайті ХНЕУ ім. С. Кузнеця за посиланням <a href="https://www.hneu.edu.ua/normatyvni-dokumenty/">https://www.hneu.edu.ua/normatyvni-dokumenty/</a>
<b>Обмеження щодо форм навчання</b>	Немає
<b>Освітня кваліфікація</b>	Бакалавр з кібербезпеки
<b>Кваліфікація(-ї) професійна(-і)</b>	Відсутня
<b>Кваліфікація в дипломі</b>	Ступінь вищої освіти – Бакалавр Спеціальність – 125 Кібербезпека Освітня програма – Кібербезпека
<b>Мета освітньої програми</b>	Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки, а також технологій цифрової економіки.
<b>Фокус та особливості (унікальність) програми</b>	Особливістю ОПІ Кібербезпека є орієнтація на сучасні вимоги до фахівців в галузі інформаційних технологій, та набуття здобувачами вищої освіти конкурентоспроможних компетентностей на основі синергізму отримання результатів навчання з інформаційної та/або кібербезпеки та програмування.

**ПРОЕКТ освітньої програми для обговорення на 2023-2024 навчальний рік**

<p><b>Опис предметної області</b></p>	<p><b>Об'єкт вивчення:</b></p> <ul style="list-style-type: none"> <li>– об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології;</li> <li>– технології забезпечення безпеки інформації;</li> <li>– процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту.</li> </ul> <p><b>Цілі навчання:</b> підготовка фахівців здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки.</p> <p><b>Теоретичний зміст предметної області</b> включає знання:</p> <ul style="list-style-type: none"> <li>– законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;</li> <li>– принципів супроводу систем та комплексів інформаційної та/або кібербезпеки;</li> <li>– теорії, моделей та принципів управління доступом до інформаційних ресурсів;</li> <li>– теорії систем управління інформаційною та/або кібербезпекою;</li> <li>– методів та засобів виявлення, управління та ідентифікації ризиків;</li> <li>– методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації;</li> <li>– методів та засобів технічного та криптографічного захисту інформації;</li> <li>– сучасних інформаційно-комунікаційних технологій;</li> <li>– сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій;</li> <li>– автоматизованих систем проектування</li> </ul> <p><b>Методи, методики та технології:</b> Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/або кібербезпеки.</p> <p><b>Інструментарій та обладнання:</b> системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/або кібербезпеки;</p> <ul style="list-style-type: none"> <li>– сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;</li> <li>– спеціалізований клас (кіберполігон).</li> </ul>
<p><b>Академічна мобільність</b></p>	<p>-</p>
<p><b>Академічні права</b></p>	<p>Можливість продовжити навчання за освітньою програмою ступеня магістра.</p>
<p><b>Професійні права</b></p>	<p><b>Знання і розуміння:</b></p> <ul style="list-style-type: none"> <li>– ґрунтовна математична підготовка в галузі захисту інформації, криптології та криптографії, теорії, моделей та принципів управління доступом до інформаційних ресурсів;</li> <li>– базові знання принципів супроводу систем та комплексів інформаційної та/або кібербезпеки та систем управління інформаційною та/або кібербезпекою;</li> <li>– методів та засобів виявлення, управління та ідентифікації ризиків, а також технічного та криптографічного захисту інформації;</li> </ul>

**ПРОЕКТ освітньої програми для обговорення на 2023-2024 навчальний рік**

	<p>– знання мов та парадигм програмування, технологій програмування, WEB- технологій, операційних систем;</p> <p>– знання методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації.</p> <p><b>Застосування знань і розумінь:</b></p> <p>– здатність використання інформаційних і комунікаційних технологій з метою пошуку нової інформації, створення баз даних, аналізу розподілених АС та їх оптимізації;</p> <p>– здатність здійснювати проектування (розробку) систем, технологій і засобів інформаційної безпеки;</p> <p>– здатність здійснювати протидію несанкціонованому проникненню в ІТ системи і мережі;</p> <p>– здатність прогнозувати, виявляти та оцінювати стан інформаційної безпеки об’єктів і систем;</p> <p>– здатність відновлювати нормальне функціонування ІТ систем і мереж після здійснення кібернападів, збоїв та відмов;</p> <p>– здатність виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту обробки інформації в ІТС;</p> <p>– здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою.</p> <p><b>Формування суджень:</b></p> <p>– вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;</p> <p>– здатність виконувати моніторинг даних, комп’ютерних зловживань та аномалій;</p> <p>– здатність до пошуку, оброблення та аналізу інформації;</p> <p>– здатність до роботи в команді;</p> <p>– здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності.</p>
<b>Працевлаштування випускників</b>	<p>Професії, на підготовку з яких спрямована ОП (згідно з чинною редакцією Національного класифікатора України: Класифікатор професій ДК 003:2010)</p> <p>1495 Менеджери (управителі) систем з інформаційної безпеки, 2149.2 Фахівець (сфера захисту інформації), 3119 Технік (сфера захисту інформації), 2131.2 Адміністратор бази даних, 2131.2 Адміністратор даних, 2131.2 Адміністратор доступу, 2131.2 Адміністратор доступу (груповий), 2132.2 Інженер-програміст.</p>

**II – ПЕРЕЛІК КОМПЕТЕНТНОСТЕЙ ВИПУСКНИКА**

<b>Інтегральна компетентність</b>	Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
<b>Загальні компетентності</b>	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії.

**ПРОЕКТ освітньої програми для обговорення на 2023-2024 навчальний рік**

	<p>КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.</p> <p>КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p>КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.</p> <p>КЗ 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.</p> <p>КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.</p>
<p><b>Спеціальні (фахові, предметні) компетентності</b></p>	<p>КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.</p> <p>КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.</p> <p>КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.</p> <p>КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.</p> <p>КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-</p>

## ПРОЕКТ освітньої програми для обговорення на 2023-2024 навчальний рік

	телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки
--	---

З метою забезпечення кореляції визначених компетентностей з класифікацією компетентностей НРК використовується матриця відповідності визначених компетентностей та дескрипторів НРК, яка є інформаційним додатком (Таблиця 1 Пояснювальної записки).

### III – НОРМАТИВНИЙ ЗМІСТ ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ, СФОРМУЛЬОВАНИЙ У ТЕРМІНАХ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗА СПЕЦІАЛЬНІСТЮ 125 КІБЕРБЕЗПЕКА

РН1 – 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 задач та 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 задач професійної діяльності;

РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

РН 5 – адаптуватися в умовах часткої 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, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;

РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;

РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;

РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;

РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;

РН 12 – розробляти моделі загроз та порушника;

РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;



## **ПРОЕКТ освітньої програми для обговорення на 2023-2024 навчальний рік**

РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;

РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;

РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;

РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;

РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;

РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;

РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;

РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;

РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);

РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;

РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту



## **ПРОЕКТ освітньої програми для обговорення на 2023-2024 навчальний рік**

інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;

РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;

РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки;

РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;

РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;

РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;

РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;

РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;

РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;

РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки;

РН 36 – виявляти небезпечні сигнали технічних засобів;

РН 37 – вимірювати параметри небезпечних та заводових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витoku технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;

РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних 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 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;

**ПРОЕКТ освітньої програми для обговорення на 2023-2024 навчальний рік**

РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;

РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;

РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;

РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;

РН 45 – застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;

РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;

РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;

РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;

РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;

РН 50 – забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);

РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;

РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;

РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз;

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

**ПРОЕКТ освітньої програми для обговорення на 2023-2024 навчальний рік****IV. СТРУКТУРА ОСВІТНЬОЇ ПРОГРАМИ ПІДГОТОВКИ  
БАКАЛАВРІВ****4.1. СТРУКТУРА ПРОГРАМИ ТА ОСВІТНІ КОМПОНЕНТИ**

<b>№</b>	<b>Освітні компоненти (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)</b>	<b>Кредити ЄКТС</b>	<b>Структура, %</b>
<b>ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ</b>			
1	<i>ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ</i>	24	10
2	<i>ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ</i>	25	10
<b>ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ</b>			
3	<i>ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ</i>	156	65
4	<i>ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ</i>	35	15
<b>ЗАГАЛЬНА КІЛЬКІСТЬ :</b>		<b>240</b>	<b>100%</b>
<i>в тому числі: вибіркова складова</i>		60	25
<b>Код ОК</b>	<b>Освітні компоненти (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)</b>	<b>Кредити ЄКТС</b>	<b>Форми підсумкового контролю</b>
<b>ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ</b>			
<i>ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ</i>			
<b>ОК1</b>	Українська мова (за професійним спрямуванням)	3	ЗАЛІК
<b>ОК2</b>	Іноземна мова (за професійним спрямуванням)	9	ЗАЛІК, ЕКЗАМЕН
<b>ОК3</b>	Соціальна та економічна історія України	4	ЗАЛІК
<b>ОК4</b>	Безпека життєдіяльності та охорона праці	3	ЗАЛІК
<b>ОК5</b>	Філософія	5	ЕКЗАМЕН
<i>ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ</i>			
<b>ВК1</b>	Навчальна дисципліна правового спрямування	5	ЗАЛІК
<b>ВК2</b>	Майнор або вільний майнор	5	ЗАЛІК
<b>ВК3</b>	Майнор або вільний майнор	5	ЗАЛІК
<b>ВК4</b>	Майнор або вільний майнор	5	ЗАЛІК
<b>ВК5</b>	Майнор або вільний майнор	5	ЗАЛІК
<b>ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ</b>			
<i>ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ</i>			
<b>ОК6</b>	Вступ до фаху	6	ЗАЛІК
<b>ОК7</b>	Інформаційна безпека держави	5	ЕКЗАМЕН
<b>ОК8</b>	Основи програмування	6	ЕКЗАМЕН

**ПРОЕКТ освітньої програми для обговорення на 2023-2024 навчальний рік**

<b>OK9</b>	Вища математика	15	ЗАЛІК, ЕКЗАМЕН
<b>OK10</b>	Розробка та аналіз алгоритмів	5	ЕКЗАМЕН
<b>OK11</b>	Фізичні основи технічних засобів розвідки	4	ЗАЛІК
<b>OK12</b>	Математичні основи криптології	4	ЗАЛІК
<b>OK13</b>	Основи побудови та захисту сучасних операційних систем	5	ЕКЗАМЕН
<b>OK14</b>	Введення в мережі	5	ЕКЗАМЕН
<b>OK15</b>	Технології програмування	12	ЗАЛІК, ЕКЗАМЕН
<b>OK16</b>	Теоретичні основи криптографії	5	ЕКЗАМЕН
<b>OK17</b>	Основи побудови та захисту мікропроцесорних систем	4	ЗАЛІК
<b>OK18</b>	Менеджмент інформаційної безпеки	5	ЕКЗАМЕН
<b>OK19</b>	Основи математичного моделювання	4	ЗАЛІК
<b>OK20</b>	Основи криптографічного захисту	5	ЗАЛІК
<b>OK21</b>	Безпека в інформаційно-комунікаційних системах	5	ЕКЗАМЕН
<b>OK22</b>	Інформаційні системи та Інтернет технології	12	ЕКЗАМЕН, ЕКЗАМЕН
<b>OK23</b>	Безпека Інтернет-речей	6	ЕКЗАМЕН
<b>OK24</b>	Виробнича практика	3	ЗВІТ
<b>OK25</b>	Комплексні системи захисту інформації	5	ЗАЛІК
<b>OK26</b>	Іноземна мова академічної та професійної комунікації	4	ЗАЛІК
<b>OK27</b>	Комплексний курсовий проект	3	КОНСУЛЬТАЦІЙ НИЙ ПРОЕКТ
<b>OK28</b>	Основи стеганографічного захисту інформації	4	ЗАЛІК
<b>OK29</b>	Організаційне забезпечення захисту інформації	4	ЗАЛІК
<b>OK30</b>	Комплексний тренінг	5	ЗВІТ
<b>OK31</b>	Переддипломна практика	5	ЗВІТ
<b>OK32</b>	Дипломний проект	10	ДИПЛОМНИЙ ПРОЕКТ
<i>ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ</i>			
<b>ВК6</b>	Мейджор 1	5	ЕКЗАМЕН
<b>ВК7</b>	Мейджор 2	5	ЕКЗАМЕН
<b>ВК8</b>	Мейджор 3	5	ЕКЗАМЕН
<b>ВК9</b>	Мейджор 4	5	ЕКЗАМЕН

## **ПРОЕКТ освітньої програми для обговорення на 2023-2024 навчальний рік**

<b>ВК10</b>	Мейджор 5	5	ЕКЗАМЕН
<b>ВК11</b>	Мейджор 6	5	ЕКЗАМЕН
<b>ВК12</b>	Мейджор 7	5	ЕКЗАМЕН

### **4.2. ВИБІРКОВА СКЛАДОВА ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ**

Вибіркова складова освітньо-професійної програми складається з:

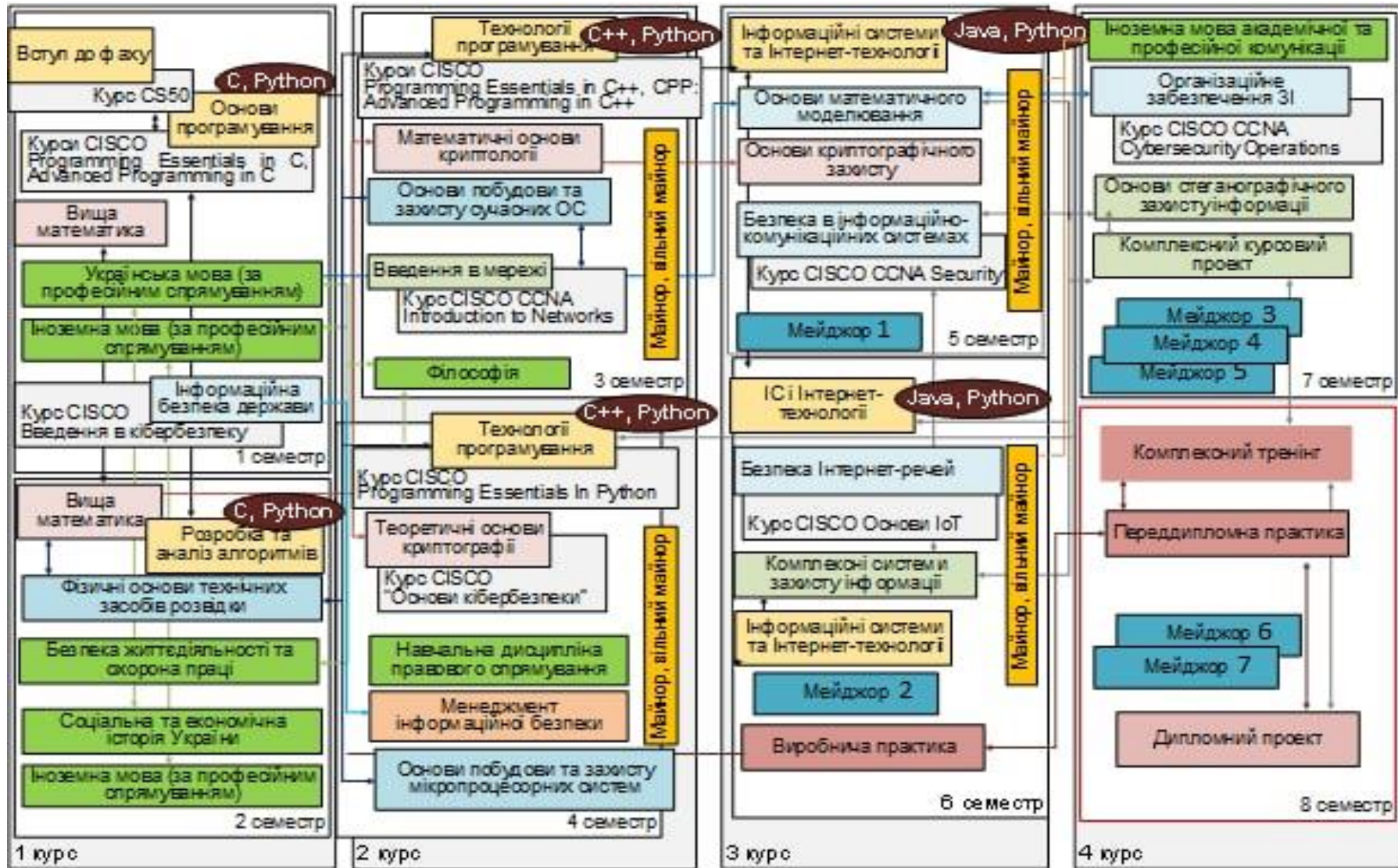
**МАЙНОРИВ** – блок взаємопов'язаних непрофільних навчальних дисциплін або **ВІЛЬНИЙ МАЙНОР** – окремі непрофільні навчальні дисципліни для створення власного **МАЙНОРУ** із загального переліку Університету (загально-університетський пул) для освітньо-кваліфікаційного рівня бакалавр. Дисципліни **МАЙНОРИВ** є обов'язковими для вибору здобувачами вищої освіти і входять до загального обсягу кредитів ЄКТС за освітньо-професійною програмою підготовки бакалаврів.

**МЕЙДЖОР** – профільні навчальні дисципліни освітньо-професійної програми, які поглиблюють професійну підготовку за певною спеціалізацією. Окрема дисципліна з обсягом 5 кредитів ЄКТС.

Дисципліна правового спрямування – окрема дисципліна з обсягом 5 кредитів ЄКТС. Загальний обсяг **МАЙНОРИВ** складає 20 кредитів ЄКТС (по 5 кредитів на дисципліну). Загальний обсяг **МЕЙДЖЕРІВ** складає 35 кредитів ЄКТС.



### 4.3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ



## **V. ФОРМИ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ**

<b>Форми атестації здобувачів вищої освіти</b>	Атестація за освітньою програмою здійснюється екзаменаційною комісією відповідно до вимог стандарту вищої освіти після виконання студентом навчального плану у формі публічного захисту кваліфікаційної роботи бакалавра (дипломного проекту) за спеціальністю 125 Кібербезпека (денна форма, заочна форма). До атестації допускаються студенти, які виконали всі вимоги освітньої програми та навчального плану.
<b>Вимоги до кваліфікаційної роботи (дипломного проекту)</b>	Атестація осіб, які здобувають ступінь бакалавра, здійснюється екзаменаційною комісією (ЕК), до складу якої можуть включатися представники роботодавців та їх об'єднань. Атестація здійснюється відкрито і публічно. Дипломний проект – це робота здобувача, яка виконується на завершальному етапі здобуття кваліфікації бакалавра з кібербезпеки для встановлення відповідності отриманих здобувачами вищої освіти результатів навчання (компетентностей) вимогам освітньої програми. Вона є кваліфікаційним документом, на підставі якого ЕК визначає рівень теоретичної підготовки випускника, його готовність до самостійної роботи за фахом і приймає рішення щодо присвоєння відповідної кваліфікації та видачу диплома. Дипломний проект є інструментом закріплення та демонстрації сформованих упродовж навчання загальних та спеціальних компетентностей відповідно до освітньо-професійної програми.
<b>Вимоги до публічного захисту</b>	У процесі публічного захисту кандидат на присвоєння бакалаврського ступеня повинен показати уміння чітко і упевнено викладати зміст проведених досліджень, аргументовано відповідати на запитання та вести дискусію. Доповідь здобувача вищої освіти повинна супроводжуватися презентаційними матеріалами та пояснювальною запискою, призначеними для загального перегляду.

## **VI. ВИМОГИ ДО НАЯВНОСТІ СИСТЕМИ ВНУТРІШНЬОГО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ**

Визначаються відповідно до Європейських стандартів та рекомендацій щодо забезпечення якості вищої освіти (ESG) та статті 16 Закону України “Про вищу освіту”.

<b>Політика щодо забезпечення якості вищої освіти</b>	Основні принципи внутрішнього забезпечення якості освіти у ХНЕУ ім. С. Кузнеця: відповідальності; відповідності; адекватності; автономності; вимірюваності; академічної культури; відкритості. Основні процедури внутрішнього забезпечення якості освіти в ХНЕУ ім. С. Кузнеця: формалізація політики якості, стратегічних цілей, завдань постійного поліпшення якості; забезпечення публічності інформації про освітні програми,
---	--



**ПРОЕКТ освітньої програми для обговорення на 2023-2024 навчальний рік**

	<p>ступені вищої освіти та кваліфікації; забезпечення дотримання академічної доброчесності працівниками закладів вищої освіти та здобувачами вищої освіти; підготовка та проведення маркетингово-моніторингових та соціально-психологічних досліджень для визначення потреб ринку праці, вимог стейкхолдерів вищої освіти, якості надання освітніх послуг і задоволеності якістю освітньої діяльності та якістю освіти; залучення стейкхолдерів вищої освіти (здобувачів вищої освіти, роботодавців, представників академічної спільноти тощо) до прийняття рішень за напрямками внутрішнього забезпечення якості; зовнішнє оцінювання якості діяльності ХНЕУ ім. С. Кузнеця за результатами участі в національних та міжнародних рейтингах вищих навчальних закладів, виконання Ліцензійних вимог, акредитації.</p> <p>Напрями: розроблення, затвердження, моніторинг та періодичний перегляд освітніх програм; забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників; забезпечення студентоцентрованого навчання, викладання та оцінювання здобувачів вищої освіти; забезпечення наявності необхідних ресурсів для організації освітнього процесу; забезпечення наявності інформаційних систем для ефективного управління освітнім процесом.</p>
<p><b>Забезпечення якості розроблення, затвердження, моніторингу, перегляду та оновлення освітніх програм</b></p>	<p>Моніторинг та періодичний перегляд освітніх програм здійснюється згідно з діючими нормативними актами в ХНЕУ ім. С. Кузнеця.</p> <p>Перегляд освітніх програм здійснюється на основі аналізу задоволення освітніх потреб здобувачів вищої освіти: можливості побудови індивідуальної траєкторії навчання, дотримання академічних свобод в освітньому процесі, задоволеності якістю освітньої програми, тощо; роботодавців: якості формування загальних та фахових компетентностей, актуальних та соціальних навичок (soft skills); інших стейкхолдерів.</p> <p>Для перегляду освітніх програм використовуються: онлайн опитування, проведення дослідження фокус-групи, аналіз документів, аналіз ситуації, самооцінка робочою групою відповідно до вимог щодо структури та змісту освітньої програми.</p> <p>Періодичність перегляду освітніх програм здійснюється: а) щорічно за результатами моніторингу; б) після завершення освітньої програми здобувачами вищої освіти, в) в разі зміни законодавчої та нормативної бази.</p>
<p><b>Забезпечення зарахування, досягнення, визнання та атестація здобувачів</b></p>	<p>Оцінювання здобувачів вищої освіти є послідовним, прозорим та проводиться відповідно до встановлених в Університеті процедур згідно з нормативними актами.</p> <p>Щорічне оцінювання здобувачів освіти здійснюється відповідно до визначених освітньою програмою форм контролю; порядку оцінювання результатів навчання, що висвітлюється в робочих програмах навчальних дисциплін, робочих планах (технологічних картах) навчальних дисциплін, силабусах навчальних дисциплін; обліку результатів навчання, який ведеться з використанням програмного забезпечення</p>

**ПРОЕКТ освітньої програми для обговорення на 2023-2024 навчальний рік**

	<p>корпоративної інформаційної системи управління (електронний журнал) та інформаційного середовища Персональної навчальної системи (ПНС) Університету. Оприлюднення результатів успішності, оцінювання результатів навчання відбувається через звіт «Інформація про поточну успішність та відвідування занять за навчальними дисциплінами семестру» (сайт Університету) та на сайті Персональних навчальних систем. Оцінювання здобувачів вищої освіти здійснюється на основі 100-бальної накопичувальної бально-рейтингової системи.</p>
<b>Забезпечення якості студентоцентрованого навчання, викладання та оцінювання</b>	<p>Планування, розподіл та надання навчальних ресурсів і забезпечення підтримки здобувачів вищої освіти враховують їх потреби та принципи студентоцентрованого навчання. Внутрішнє забезпечення якості вищої освіти гарантує, що всі необхідні ресурси відповідають цілям навчання, є загальнодоступними, а здобувачі вищої освіти поінформовані про їх наявність.</p>
<b>Забезпечення якості науково-педагогічних працівників</b>	<p>Щорічне рейтингове оцінювання діяльності науково-педагогічних працівників, кафедр і факультетів Університету здійснюється за рахунок використання механізмів оцінювання та самооцінювання результативності науково-педагогічної діяльності, її спрямованості на пріоритети розвитку національної системи вищої освіти, стратегії розвитку Університету, особистісного професійного розвитку науково-педагогічних працівників. Підсумки рейтингового оцінювання підводяться за результатами діяльності, досягнутими протягом навчального року. Оприлюднення результатів щорічного оцінювання науково-педагогічних працівників, кафедр та факультетів відбувається на засіданні вченої ради Університету.</p>
<b>Ресурсне забезпечення освітнього процесу (навчальні ресурси та підтримка здобувачів вищої освіти)</b>	<p>Заклад вищої освіти забезпечує освітній процес необхідними та доступними ресурсами (кадровими, методичними, матеріальними, інформаційними та ін.) та здійснює відповідну підтримку здобувачів вищої освіти. Організаційно-методична підтримка самостійної роботи здобувачів вищої освіти полягає у розробці методичних, дидактичних, інструктивних матеріалів, наданні можливості формувати, закріплювати, поглиблювати й систематизувати отримані під час аудиторних занять знання та вміння, здійснювати самопідготовку й самоконтроль опанування освітньої-професійної програми та реалізується через Персональну навчальну систему ХНЕУ ім. С. Кузнеця.</p>
<b>Інформаційне забезпечення (інформаційний менеджмент)</b>	<p>З метою управління освітнім процесом розроблено ефективну політику в сфері інформаційного менеджменту та відповідну інтегровану інформаційну систему управління освітнім процесом. Дана система передбачає автоматизацію основних функцій управління освітнім процесом, зокрема: забезпечення проведення вступної кампанії, планування та організацію освітнього процесу; доступ до навчальних ресурсів; облік та аналіз успішності здобувачів вищої освіти; адміністрування основних та допоміжних процесів забезпечення освітньої діяльності; управління кадрами та ін.</p>

**ПРОЕКТ освітньої програми для обговорення на 2023-2024 навчальний рік**

<p><b>Публічність інформації про освітні програми, освітню, наукову діяльність</b></p>	<p>Достовірна, об'єктивна, актуальна, своєчасна та легкодоступна інформація за освітньо-професійною програмою публікується на сайті ХНЕУ ім. С. Кузнеця, включаючи програми для потенційних здобувачів вищої освіти, випускників, інших стейкхолдерів і громадськості.</p> <p>Публічною є інформація про освітню діяльність за спеціальністю, включаючи критерії відбору на навчання; заплановані результати навчання за цією програмою; процедури навчання, викладання та оцінювання, що використовуються тощо.</p>
<p><b>Забезпечення академічної доброчесності</b></p>	<p>Забезпечення запобігання та виявлення академічного плагіату у наукових працях працівників закладу вищої освіти та здобувачів вищої освіти реалізується через політику, стандарти і процедури дотримання академічної доброчесності, регулюється такими документами ХНЕУ ім. С. Кузнеця: Кодекс академічної доброчесності; Кодекс професійної етики та організаційної культури працівників і здобувачів вищої освіти ХНЕУ ім. С. Кузнеця; Положення про комісію з питань академічної доброчесності ХНЕУ ім. С. Кузнеця.</p> <p>Перевірка наукових праць науково-педагогічних працівників Університету та здобувачів вищої освіти здійснюється за допомогою інтернет-сервісів на основі відкритих інтернет-ресурсів та системи StrikePlagiarism.com, що діє на підставі Ліцензійного Договору про надання права користування антиплагіатним програмним забезпеченням.</p>

**ПОЯСНЮВАЛЬНА ЗАПИСКА**

Матриця відповідності визначених компетентностей дескрипторам НРК та матриця відповідності визначених результатів навчання та компетентностей представлені в Таблицях 1 і 2.

**Таблиця 1**  
**Матриця відповідності визначених компетентностей дескрипторам НРК**

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
<b>ЗАГАЛЬНІ КОМПЕТЕНТНОСТІ</b>				
КЗ 1. Здатність застосовувати знання у практичних ситуаціях.	+	+		
КЗ 2. Знання та розуміння предметної області та розуміння професії.	+	+		
КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово	+	+	+	
КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням	+	+	+	+
КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.	+	+		+
КЗ 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		+	+	+
КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.		+	+	+
<b>СПЕЦІАЛЬНІ (ФАХОВІ) КОМПЕТЕНТНОСТІ</b>				
КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.		+		+
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.	+	+		+

**ПРОЕКТ освітньої програми для обговорення на 2023-2024 навчальний рік**

<b>Класифікація компетентностей за НРК</b>	<b>Знання</b>	<b>Уміння</b>	<b>Комунікація</b>	<b>Автономія та відповідальність</b>
КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.	+	+		+
КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.	+	+	+	
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	+	+		+
КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.	+	+	+	
КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)	+		+	
КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.	+	+		+
КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.	+	+	+	
КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.	+	+	+	
КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	+	+		+
КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки	+	+		+











Результати навчання	Компетентності																			
	Загальні							Спеціальні (фахові)												
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12	
РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем	OK1 OK4 OK5 OK7 OK9 OK11 OK12 OK14 OK16 OK17 OK20 OK21 OK22 OK23 OK24 OK31 OK32								OK1 OK4 OK5 OK9 OK7 OK11 OK12 OK14 OK16 OK17 OK20 OK21 OK22 OK23 OK24 OK31 OK32											OK1 OK4 OK5 OK9 OK7 OK11 OK12 OK14 OK16 OK17 OK20 OK21 OK22 OK23 OK24 OK31 OK32
РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах	OK1 OK4 OK5 OK7 OK9 OK11 OK12 OK14 OK16 OK17 OK20 OK21 OK22 OK23 OK24 OK32								OK1 OK4 OK5 OK7 OK9 OK11 OK12 OK14 OK16 OK17 OK20 OK21 OK22 OK23 OK24 OK32											OK1 OK4 OK5 OK7 OK9 OK11 OK12 OK14 OK16 OK17 OK20 OK21 OK22 OK23 OK24 OK32
РН 12 – розробляти моделі загроз та порушника													OK8 OK10 OK11 OK14 OK15 OK19							OK8 OK10 OK11 OK14 OK15 OK19

Результати навчання	Компетентності																			
	Загальні							Спеціальні (фахові)												
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12	
														OK21 OK22					OK21 OK22	
РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних					OK4 OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK19 OK20 OK21 OK22 OK30 OK31 OK32				OK4 OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK19 OK20 OK21 OK22 OK30 OK31 OK32				OK4 OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK19 OK20 OK21 OK22 OK30 OK31 OK32						OK4 OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK19 OK20 OK21 OK22 OK30 OK31 OK32	OK4 OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK19 OK20 OK21 OK22 OK30 OK31 OK32
РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень									OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK23 OK30 OK31 OK32	OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK23 OK30 OK31 OK32		OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK23 OK30 OK31 OK32					OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK23 OK30 OK31 OK32	OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK23 OK30 OK31 OK32	OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK23 OK30 OK31 OK32	
РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій									OK7 OK9 OK11 OK12 OK14	OK7 OK9 OK11 OK12 OK14								OK7 OK9 OK11 OK12 OK14		

Результати навчання	Компетентності																			
	Загальні							Спеціальні (фахові)												
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12	
									OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK23	OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK23									OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK23	
PH 16 – реалізувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів								OK7 OK8 OK9 OK10 OK11 OK12 OK14 OK15 OK16 OK18 OK19 OK20 OK22 OK27 OK29		OK7 OK8 OK9 OK10 OK11 OK12 OK14 OK15 OK16 OK18 OK19 OK20 OK22 OK27 OK29				OK7 OK8 OK9 OK10 OK11 OK12 OK14 OK15 OK16 OK18 OK19 OK20 OK22 OK27 OK29						OK7 OK8 OK9 OK10 OK11 OK12 OK14 OK15 OK16 OK18 OK19 OK20 OK22 OK27 OK29
PH 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків,		OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14 OK15 OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK23							OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14 OK15 OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK23	OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14 OK15 OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK23	OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14 OK15 OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK23	OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14 OK15 OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK23	OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14 OK15 OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK23						OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14 OK15 OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK23	

Результати навчання	Компетентності																			
	Загальні							Спеціальні (фахові)												
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12	
процесів для внутрішніх і віддалених компонент		OK25 OK27 OK29 OK30 OK31 OK32							OK25 OK27 OK29 OK30 OK31 OK32	OK25 OK27 OK29 OK30 OK31 OK32	OK25 OK27 OK29 OK30 OK31 OK32	OK25 OK27 OK29 OK30 OK31 OK32	OK25 OK27 OK29 OK30 OK31 OK32		OK25 OK27 OK29 OK30 OK31 OK32				OK25 OK27 OK29 OK30 OK31 OK32	
PH 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів	OK1 OK4 OK5 OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK23 OK24 OK31 OK32							OK1 OK4 OK5 OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK23 OK24 OK31 OK32	OK1 OK4 OK5 OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK23 OK24 OK31 OK32			OK1 OK4 OK5 OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK23 OK24 OK31 OK32							OK1 OK4 OK5 OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK23 OK24 OK31 OK32	
PH 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах	OK1 OK4 OK5 OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK20 OK21 OK22							OK1 OK4 OK5 OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK20 OK21 OK22				OK1 OK4 OK5 OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK20 OK21 OK22			OK1 OK4 OK5 OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK20 OK21 OK22					OK1 OK4 OK5 OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK20 OK21 OK22

Результати навчання	Компетентності																					
	Загальні							Спеціальні (фахові)														
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12			
	OK23 OK24 OK31 OK32								OK23 OK24 OK31 OK32			OK23 OK24 OK31 OK32			OK23 OK24 OK31 OK32			OK22 OK23 OK24 OK31 OK32				
РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах	OK1 OK4 OK5 OK7 OK9 OK11 OK12 OK13 OK14 OK15 OK16 OK18 OK19 OK20 OK21 OK22 OK23 OK24 OK30 OK31 OK32								OK1 OK4 OK5 OK7 OK9 OK11 OK12 OK13 OK14 OK15 OK16 OK18 OK19 OK20 OK21 OK22 OK23 OK24 OK30 OK31 OK32	OK1 OK4 OK5 OK7 OK9 OK11 OK12 OK13 OK14 OK15 OK16 OK18 OK19 OK20 OK21 OK22 OK23 OK24 OK30 OK31 OK32			OK1 OK4 OK5 OK7 OK9 OK11 OK12 OK13 OK14 OK15 OK16 OK18 OK19 OK20 OK21 OK22 OK23 OK24 OK30 OK31 OK32	OK1 OK4 OK5 OK7 OK9 OK11 OK12 OK13 OK14 OK15 OK16 OK18 OK19 OK20 OK21 OK22 OK23 OK24 OK30 OK31 OK32			OK1 OK4 OK5 OK7 OK9 OK11 OK12 OK13 OK14 OK15 OK16 OK18 OK19 OK20 OK21 OK22 OK23 OK24 OK30 OK31 OK32			OK1 OK4 OK5 OK7 OK9 OK11 OK12 OK13 OK14 OK15 OK16 OK18 OK19 OK20 OK21 OK22 OK23 OK24 OK30 OK31 OK32		
РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах	OK1 OK4 OK5 OK7 OK9 OK12 OK13 OK16 OK18 OK20 OK21 OK22 OK24 OK27											OK1 OK4 OK5 OK7 OK9 OK12 OK13 OK16 OK18 OK20 OK21 OK22 OK24 OK27			OK1 OK4 OK5 OK7 OK9 OK12 OK13 OK16 OK18 OK20 OK21 OK22 OK24 OK27			OK1 OK4 OK5 OK7 OK9 OK12 OK13 OK16 OK18 OK20 OK21 OK22 OK24 OK27			OK1 OK4 OK5 OK7 OK9 OK12 OK13 OK16 OK18 OK20 OK21 OK22 OK24 OK27	



Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
	OK28 OK31 OK32											OK28 OK31 OK32				OK28 OK31 OK32			OK28 OK31 OK32
РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки	OK1 OK4 OK5 OK7 OK9 OK12 OK13 OK16 OK20 OK24 OK31 OK32											OK1 OK4 OK5 OK7 OK9 OK12 OK13 OK16 OK20 OK24 OK31 OK32							OK1 OK4 OK5 OK7 OK9 OK12 OK13 OK16 OK20 OK24 OK31 OK32
РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах												OK7 OK9 OK12 OK13 OK14 OK15 OK16 OK17 OK20 OK21 OK22	OK7 OK9 OK12 OK13 OK14 OK15 OK16 OK17 OK20 OK21 OK22		OK7 OK9 OK12 OK13 OK14 OK15 OK16 OK17 OK20 OK21 OK22				OK7 OK9 OK12 OK13 OK14 OK15 OK16 OK17 OK20 OK21 OK22
РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових)	OK1 OK4 OK5 OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK16 OK18 OK20 OK21										OK1 OK4 OK5 OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK16 OK18 OK20 OK21	OK1 OK4 OK5 OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK16 OK18 OK20 OK21			OK1 OK4 OK5 OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK16 OK18 OK20 OK21			OK1 OK4 OK5 OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK16 OK18 OK20 OK21	

Результати навчання	Компетентності																			
	Загальні							Спеціальні (фахові)												
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12	
	OK22 OK24 OK25 OK27 OK28 OK29 OK31 OK32										OK22 OK24 OK25 OK27 OK28 OK29 OK31 OK32	OK22 OK24 OK25 OK27 OK28 OK29 OK31 OK32				OK22 OK24 OK25 OK27 OK28 OK29 OK31 OK32				
РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту											OK7 OK9 OK12 OK13 OK16 OK18 OK20 OK21 OK22 OK28 OK32			OK7 OK9 OK12 OK13 OK16 OK18 OK20 OK21 OK22 OK28 OK32	OK7 OK9 OK12 OK13 OK16 OK18 OK20 OK21 OK22 OK28 OK32				OK7 OK9 OK12 OK13 OK16 OK18 OK20 OK21 OK22 OK28 OK32	
РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем											OK7 OK9 OK12 OK13 OK16 OK20 OK32								OK7 OK9 OK12 OK13 OK16 OK20 OK32	
РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-	OK1 OK4 OK5 OK6 OK10 OK11										OK1 OK4 OK5 OK6 OK10 OK11	OK1 OK4 OK5 OK6 OK10 OK11	OK1 OK4 OK5 OK6 OK10 OK11							

Результати навчання	Компетентності																			
	Загальні							Спеціальні (фахові)												
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12	
телекомунікаційних (автоматизованих) системах	OK12 OK13 OK14 OK15 OK16 OK17 OK20 OK21 OK22 OK24 OK25 OK27 OK29 OK31 OK32										OK12 OK13 OK14 OK15 OK16 OK17 OK20 OK21 OK22 OK24 OK25 OK27 OK29 OK31 OK32	OK12 OK13 OK14 OK15 OK16 OK17 OK20 OK21 OK22 OK24 OK25 OK27 OK29 OK31 OK32	OK12 OK13 OK14 OK15 OK16 OK17 OK20 OK21 OK22 OK24 OK25 OK27 OK29 OK31 OK32							
РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки					OK4 OK7 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK27 OK28 OK30 OK31 OK32						OK4 OK7 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK27 OK28 OK30 OK31 OK32	OK4 OK7 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK27 OK28 OK30 OK31 OK32			OK4 OK7 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK27 OK28 OK30 OK31 OK32				OK7 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK27 OK28 OK30 OK31 OK32	
РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності										OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14	OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14	OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14			OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14	OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14			OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14	

Результати навчання	Компетентності																				
	Загальні							Спеціальні (фахові)													
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12		
використання комплексів засобів захисту в умовах реалізації загроз різних класів										OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32	OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32	OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32			OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32	OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32					OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32
РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем																				OK11 OK14 OK19 OK22	
РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем									OK11 OK12 OK14 OK15 OK16 OK17 OK20 OK21 OK22 OK23 OK30 OK31 OK32				OK11 OK12 OK14 OK15 OK16 OK17 OK20 OK21 OK22 OK23 OK30 OK31 OK32					OK11 OK12 OK14 OK15 OK16 OK17 OK20 OK21 OK22 OK23 OK30 OK31 OK32			
РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки	OK1 OK4 OK5 OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK16										OK1 OK5 OK4 OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK16	OK1 OK4 OK5 OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK16			OK1 OK4 OK5 OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK16				OK1 OK4 OK5 OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK16		

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
	OK20										OK20	OK20			OK20			OK20	
	OK21										OK21	OK21			OK21			OK21	
	OK22										OK22	OK22			OK22			OK22	
	OK24										OK25	OK24			OK24			OK24	
	OK25										OK24	OK25			OK25			OK25	
	OK27										OK27	OK27			OK27			OK27	
	OK29										OK29	OK29			OK29			OK29	
	OK31										OK31	OK31			OK31			OK31	
	OK32										OK32	OK32			OK32			OK32	
РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків								OK6			OK6			OK6	OK6			OK6	OK6
								OK7			OK7			OK7	OK7			OK7	OK7
								OK10			OK10			OK10	OK10			OK10	OK10
								OK11			OK11			OK11	OK11			OK11	OK11
								OK14			OK14			OK14	OK14			OK14	OK14
								OK18			OK18			OK18	OK18			OK18	OK18
								OK19			OK19			OK19	OK19			OK19	OK19
								OK21			OK21			OK21	OK21			OK21	OK21
								OK22			OK22			OK22	OK22			OK22	OK22
								OK25			OK25			OK25	OK25			OK25	OK25
								OK27			OK27			OK27	OK27			OK27	OK27
								OK28			OK28			OK28	OK28			OK28	OK28
								OK29			OK29			OK29	OK29			OK29	OK29
								OK32			OK32			OK32	OK32			OK32	OK32
РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації								OK6			OK6	OK6			OK6	OK6			OK6
								OK7			OK7	OK7			OK7	OK7			OK7
								OK10			OK10	OK10			OK10	OK10			OK10
								OK11			OK11	OK11			OK11	OK11			OK11
								OK12			OK12	OK12			OK12	OK12			OK12
								OK13			OK13	OK13			OK13	OK13			OK13
								OK14			OK14	OK14			OK14	OK14			OK14
								OK16			OK16	OK16			OK16	OK16			OK16
								OK18			OK18	OK18			OK18	OK18			OK18
								OK19			OK19	OK19			OK19	OK19			OK19
								OK20			OK20	OK20			OK20	OK20			OK20
								OK21			OK21	OK21			OK21	OK21			OK21
								OK22			OK22	OK22			OK22	OK22			OK22
								OK25			OK25	OK25			OK25	OK25			OK25
								OK27			OK27	OK27			OK27	OK27			OK27
								OK28			OK28	OK28			OK28	OK28			OK28

Результати навчання	Компетентності																			
	Загальні							Спеціальні (фахові)												
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12	
								OK29 OK32			OK29 OK32	OK29 OK32			OK29 OK32	OK29 OK32			OK29 OK32	
РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки	OK1 OK4 OK5 OK6 OK7 OK8 OK9 OK10 OK11 OK12 OK13 OK14 OK15 OK16 OK18 OK19 OK20 OK21 OK22 OK24 OK25 OK27 OK28 OK29 OK31 OK32							OK1 OK4 OK5 OK6 OK7 OK8 OK9 OK10 OK11 OK12 OK13 OK14 OK15 OK16 OK18 OK19 OK20 OK21 OK22 OK24 OK25 OK27 OK28 OK29 OK31 OK32		OK1 OK4 OK5 OK6 OK7 OK8 OK9 OK10 OK11 OK12 OK13 OK14 OK15 OK16 OK18 OK19 OK20 OK21 OK22 OK24 OK25 OK27 OK28 OK29 OK31 OK32	OK1 OK4 OK5 OK6 OK7 OK8 OK9 OK10 OK11 OK12 OK13 OK14 OK15 OK16 OK18 OK19 OK20 OK21 OK22 OK24 OK25 OK27 OK28 OK29 OK31 OK32	OK1 OK4 OK5 OK6 OK7 OK8 OK9 OK10 OK11 OK12 OK13 OK14 OK15 OK16 OK18 OK19 OK20 OK21 OK22 OK24 OK25 OK27 OK28 OK29 OK31 OK32	OK1 OK4 OK5 OK6 OK7 OK8 OK9 OK10 OK11 OK12 OK13 OK14 OK15 OK16 OK18 OK19 OK20 OK21 OK22 OK24 OK25 OK27 OK28 OK29 OK31 OK32	OK1 OK4 OK5 OK6 OK7 OK8 OK9 OK10 OK11 OK12 OK13 OK14 OK15 OK16 OK18 OK19 OK20 OK21 OK22 OK24 OK25 OK27 OK28 OK29 OK31 OK32	OK1 OK4 OK5 OK6 OK7 OK8 OK9 OK10 OK11 OK12 OK13 OK14 OK15 OK16 OK18 OK19 OK20 OK21 OK22 OK24 OK25 OK27 OK28 OK29 OK31 OK32	OK1 OK4 OK5 OK6 OK7 OK8 OK9 OK10 OK11 OK12 OK13 OK14 OK15 OK16 OK18 OK19 OK20 OK21 OK22 OK24 OK25 OK27 OK28 OK29 OK31 OK32	OK1 OK4 OK5 OK6 OK7 OK8 OK9 OK10 OK11 OK12 OK13 OK14 OK15 OK16 OK18 OK19 OK20 OK21 OK22 OK24 OK25 OK27 OK28 OK29 OK31 OK32	OK1 OK4 OK5 OK6 OK7 OK8 OK9 OK10 OK11 OK12 OK13 OK14 OK15 OK16 OK18 OK19 OK20 OK21 OK22 OK24 OK25 OK27 OK28 OK29 OK31 OK32	OK1 OK4 OK5 OK6 OK7 OK8 OK9 OK10 OK11 OK12 OK13 OK14 OK15 OK16 OK18 OK19 OK20 OK21 OK22 OK24 OK25 OK27 OK28 OK29 OK31 OK32	OK1 OK4 OK5 OK6 OK7 OK8 OK9 OK10 OK11 OK12 OK13 OK14 OK15 OK16 OK18 OK19 OK20 OK21 OK22 OK24 OK25 OK27 OK28 OK29 OK31 OK32
РН 36 – виявляти небезпечні сигнали технічних засобів																			OK30 OK31	
РН 37 – вимірювати параметри небезпечних та заводових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами													OK14 OK15 OK17 OK21 OK22 OK30 OK31 OK32						OK14 OK15 OK17 OK21 OK22 OK30 OK31 OK32	

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
відповідно до вимог нормативних документів системи технічного захисту інформації																			
РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації													OK14 OK15 OK17 OK21 OK22 OK30 OK31 OK32				OK14 OK15 OK17 OK21 OK22 OK30 OK31 OK32		
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																	OK30 OK31		
РН 40 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації																	OK30 OK31		
РН 41 – забезпечувати неперервність процесу															OK7 OK9 OK23			OK7 OK9 OK23	

Результати навчання	Компетентності																						
	Загальні							Спеціальні (фахові)															
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12				
ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур															OK31 OK32			OK31 OK32					
РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки											OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32					OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32			OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32		OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32		OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32
РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів		OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29						OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29			OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29			OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29			OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29		OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29		OK6 OK7 OK9 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29		



Результати навчання	Компетентності																			
	Загальні							Спеціальні (фахові)												
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12	
		OK30 OK31 OK32						OK30 OK31 OK32			OK30 OK31 OK32	OK30 OK31 OK32			OK30 OK31 OK32	OK30 OK31 OK32			OK30 OK31 OK32	
РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами								OK6 OK7 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32			OK6 OK7 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32	OK6 OK7 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32			OK6 OK7 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32	OK6 OK7 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32				OK6 OK7 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32
РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів											OK6 OK7 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32	OK6 OK7 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32			OK6 OK7 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32	OK6 OK7 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32				OK6 OK7 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32

Результати навчання	Компетентності																			
	Загальні							Спеціальні (фахові)												
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12	
РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах											OK6 OK7 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32	OK6 OK7 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32			OK6 OK7 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32	OK6 OK7 OK10 OK11 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK21 OK22 OK25 OK27 OK28 OK29 OK32				
РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації									OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK30 OK31 OK32	OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK30 OK31 OK32							OK7 OK9 OK11 OK12 OK13 OK14 OK16 OK17 OK18 OK19 OK20 OK21 OK22 OK30 OK31 OK32			
РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту											OK7 OK9 OK12 OK13 OK14 OK15	OK7 OK9 OK12 OK13 OK14 OK15			OK7 OK9 OK12 OK13 OK14 OK15		OK7 OK9 OK12 OK13 OK14 OK15	OK7 OK9 OK12 OK13 OK14 OK15		

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах												OK16 OK17 OK20 OK21 OK22 OK30 OK31 OK32	OK16 OK17 OK20 OK21 OK22 OK30 OK31 OK32		OK16 OK17 OK20 OK21 OK22 OK30 OK31 OK32		OK16 OK17 OK20 OK21 OK22 OK30 OK31 OK32	OK16 OK17 OK20 OK21 OK22 OK30 OK31 OK32	
РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах												OK7 OK9 OK12 OK13 OK14 OK15 OK16 OK17 OK20 OK21 OK22 OK32	OK7 OK9 OK12 OK13 OK14 OK15 OK16 OK17 OK20 OK21 OK22 OK32		OK7 OK9 OK12 OK13 OK14 OK15 OK16 OK17 OK20 OK21 OK22 OK32		OK7 OK9 OK12 OK13 OK14 OK15 OK16 OK17 OK20 OK21 OK22 OK32	OK7 OK9 OK12 OK13 OK14 OK15 OK16 OK17 OK20 OK21 OK22 OK32	
РН 50 – забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних)										OK7 OK9 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK22 OK32	OK7 OK9 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK22 OK32			OK7 OK9 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK22 OK32		OK7 OK9 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK22 OK32	OK7 OK9 OK12 OK13 OK14 OK16 OK18 OK19 OK20 OK22 OK32		
РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах												OK7 OK9 OK12 OK13 OK16 OK20 OK32	OK7 OK9 OK12 OK13 OK16 OK20 OK32		OK7 OK9 OK12 OK13 OK16 OK20 OK32		OK7 OK9 OK12 OK13 OK16 OK20 OK32	OK7 OK9 OK12 OK13 OK16 OK20 OK32	



Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
(вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні	OK4	OK4				OK4	OK4												
	OK5	OK5				OK5	OK5												
	OK6	OK6				OK6	OK6												
	OK7	OK7				OK7	OK7												
	OK12	OK12				OK12	OK12												
	OK16	OK16				OK16	OK16												
	OK18	OK18				OK18	OK18												
	OK21	OK21				OK21	OK21												
	OK22	OK22				OK22	OK22												
	OK24	OK24				OK24	OK24												
	OK25	OK25				OK25	OK25												
	OK27	OK27				OK27	OK27												
	OK29	OK29				OK29	OK29												
	OK30	OK30				OK30	OK30												
	OK31	OK31				OK31	OK31												
	OK32	OK32				OK32	OK32												

**Гарант ОП**

*підписано*

**Вячеслав ЛИМАРЕНКО**

