ПРОЕКТ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

“КІБЕРБЕЗПЕКА”

(назва ОПП /ОНП)

РІВЕНЬ ВИЩОЇ ОСВІТИ	**Перший (бакалаврський)**
СТУПІНЬ ВИЩОЇ ОСВІТИ	**Бакалавр**
ГАЛУЗЬ ЗНАНЬ	**12 Інформаційні технології**
СПЕЦІАЛЬНІСТЬ	**125 Кібербезпека**

Харків
2021

ПРОЄКТ

ПРЕАМБУЛА

Розробники ОП (Склад робочої групи) у складі:

1. Євсеєв Сергій Петрович – доктор технічних наук, професор, завідувач кафедри кібербезпеки та інформаційних технологій;
2. Король Ольга Григорівна – кандидат технічних наук, доцент, доцент кафедри кібербезпеки та інформаційних технологій.
3. Мілов Олександр Володимирович – доктор технічних наук, професор, професор кафедри кібербезпеки та інформаційних технологій.
4. Макаренко Антон Олегович – здобувач вищої освіти.
5. Ковтун Владислав Юрійович – технічний директор компанії “Сайфер”.
6. Кравченко Павел Олександрович – співзасновник Distributed Lab.

ОП розроблено/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.
3. Аналізу ринку праці, з урахуванням регіонального контексту.
4. Вивчення вітчизняного та зарубіжного досвіду.
5. Пропозицій роботодавців.
6. Рекомендації після процедур внутрішнього та зовнішнього оцінювання ОП (акредитація НАЗЯВО).

Рецензії-відгуки зовнішніх стейкхолдерів (додаються).

ПРОЄКТ

І. ЗАГАЛЬНА ХАРАКТЕРИСТИКА

Рівень вищої освіти	Перший (бакалаврський) рівень
Ступінь вищої освіти	Бакалавр
Галузі знань	12 Інформаційні технології
Спеціальності	125 Кібербезпека
Освітня програма (укр. та англ. мовою)	Кібербезпека / Cybersecurity
Форми здобуття освіти, обсяг освітньої програми в кредитах ЄКТС та терміни навчання	- на базі повної загальної середньої освіти: денна форма – 240 кредитів, 3 роки 10 місяців; заочна форма – 4 роки 10 місяців. - на базі ступеня “молодший бакалавр” (освітньо-кваліфікаційного рівня “молодший спеціаліст”): денна форма – 240 кредитів, 2 роки 10 місяців; заочна форма – 2 роки 10 місяців.
Наявність акредитації	-
Мова(и) навчання / оцінювання	українська / англійська
Структурний підрозділ відповідальний за ОП	Кафедра кібербезпеки та інформаційних технологій; Навчальна лабораторія кафедри кібербезпеки та інформаційних технологій
Вимоги до зарахування	(згідно правил прийому)
Обмеження щодо форм навчання	Не має
Освітня кваліфікація	Бакалавр з кібербезпеки
Кваліфікація(-ї) професійна(-і)	Відсутня
Кваліфікація в дипломі	Ступінь вищої освіти − Бакалавр Спеціальність – 125 Кібербезпека Освітня програма – Кібербезпека
Мета освітньої програми	підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки, а також технологій цифрової економіки.
Фокус та особливості (унікальність) програми	Особливістю програм спеціальності “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.
Опис предметної області	**Об’єкт вивчення:** – об’єкти інформатизації, включаючи комп’ютерні, автоматизовані,

	телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. **Цілі навчання:** підготовка фахівців здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області:** Знання: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або 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 проектування **Методи, методики та технології:** Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки. **Інструментарій та обладнання:** системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; – спеціалізований клас (кіберполігон).
Академічна мобільність	Угоди про співпрацю щодо реалізації програм внутрішньої академічної мобільності здобувачів вищої освіти за освітньою програмою "Кібербезпека" спеціальності 125 з Одеським національним технологічним університетом, Чернігівським національним технологічним університетом.
Академічні права	Можливість продовжити навчання за освітньою програмою ступеня магістра.
Професійні права	**Знання і розуміння:** – ґрунтовна математична підготовка в галузі захисту інформації, криптології та криптографії, теорії, моделей та принципів управління доступом до інформаційних ресурсів; – базові знання принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – базові знання систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – знання методів та засобів технічного та криптографічного захисту інформації; – знання мов та парадигм програмування, технологій програмування, WEB- технологій, операційних систем; – знання методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації.

	Застосування знань і розумінь: – здатність використання інформаційних і комунікаційних технологій з метою пошуку нової інформації, створення баз даних, аналізу розподілених АС та їх оптимізації; – здатність здійснювати проектування (розробку) систем, технологій і засобів інформаційної безпеки; – здатність здійснювати протидію несанкціонованому проникненню в ІТ системи і мережі; – здатність прогнозувати, виявляти та оцінювати стан інформаційної безпеки об'єктів і систем; – здатність відновлювати нормальне функціонування ІТ систем і мереж після здійснення кібернападів, збоїв та відмов; – здатність виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту обробки інформації в ІТС; – здатністьформувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою. **Формування суджень:** – вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням; – здатність виконувати моніторинг даних, комп'ютерних зловживань та аномалій; – здатність до пошуку, оброблення та аналізу інформації; – здатність до роботи в команді; – здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності.
Працевлаштування випускників	Професії, на підготовку з яких спрямована ОП (згідно з чинною редакцією Національного класифікатора України: Класифікатор професій ДК 003:2010) 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.

ПРОЄКТ

ІІ – ПЕРЕЛІК КОМПЕТЕНТНОСТЕЙ ВИПУСКНИКА

Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності	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.
Спеціальні (фахові, предметні) компетентності	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. 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.

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**).

ПРОЄКТ

ІІІ – 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 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, 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;

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 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 завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку 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;
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 ріні 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.

ПРОЄКТ

IV. СТРУКТУРА ОСВІТНЬОЇ ПРОГРАМИ ПІДГОТОВКИ БАКАЛАВРІВ

4.1. СТРУКТУРА ПРОГРАМИ ТА ОСВІТНІ КОМПОНЕНТИ

№	Освітні компоненти (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кредити ЄКТС	Структура, %
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
1	*ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ*	24	10
2	*ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ*	5	2
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
3	*ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ*	156	65
4	*ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ*	55	23
	ЗАГАЛЬНА КІЛЬКІСТЬ :	***240***	***100%***
	в тому числі: вибіркова складова		

Код ОК	Освітні компоненти (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кредити ЄКТС	Форми підсумкового контролю
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ			
ОК1	Українська мова (за професійним спрямуванням)	5	Екзамен
ОК2	Іноземна мова (за професійним спрямуванням)	9	Залік, Екзамен
ОК3	Соціальна та економічна історія України	5	Екзамен
ОК4	Філософія	5	Екзамен
	ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ		
ВК1	Дисципліна правового спрямування	5	Залік
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ			
ОК5	Вища математика	15	Залік, Екзамен
ОК6	Вступ до фаху	5	Залік
ОК7	Розробка та аналіз алгоритмів	5	Залік
ОК8	Фізичні основи технічних засобів розвідки	4	Залік
ОК9	Інформаційна безпека держави	5	Екзамен

ОК10	Основи програмування	5	Екзамен
ОК11	Тренінг-курс “Безпека життєдіяльності”	2	Залік
ОК12	Математичні основи криптології	4	Залік
ОК13	Теоретичні основи криптографії	5	Екзамен
ОК14	Основи побудови та захисту сучасних операційних систем	5	Екзамен
ОК15	Технології програмування	11	Залік, Екзамен
ОК16	Основи побудови та захисту мікропроцесорних систем	4	Залік
ОК17	Менеджмент інформаційної безпеки	5	Екзамен
ОК18	Курсовий проект: Введення в мережі	1	КП
ОК19	Введення в мережі	5	Екзамен
ОК20	Інформаційні системи та Інтернет технології	12	Екзамен, Екзамен
ОК21	Основи математичного моделювання	4	Залік
ОК22	Безпека Інтернет-речей	6	Екзамен
ОК23	Виробнича практика	3	ЗВІТ
ОК24	Основи криптографічного захисту	5	Залік
ОК25	Комплексні системи захисту інформації	5	Залік
ОК26	Безпека в інформаційно-комунікаційних системах	5	Екзамен
ОК27	Комплексний курсовий проект	2	КП
ОК28	Основи стеганографічного захисту інформації	5	Залік
ОК29	Тренінг-курс “Основи охорони праці”	2	Залік
ОК30	Іноземна мова академічної та професійної комунікації	4	Залік
ОК31	Організаційне забезпечення захисту інформації	4	Залік
ОК32	Комплексний тренінг	3	ЗВІТ
ОК33	Переддипломна практика	5	ЗВІТ
ОК34	Дипломний проект	10	Дипломний проект
ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ			
ВК2	Майнор або вільний майнор	5	Залік
ВК3	Майнор або вільний майнор	5	Залік
ВК4	Майнор або вільний майнор	5	Залік
ВК5	Майнор або вільний майнор	5	Залік
ВК6	Мейджор 1	5	Екзамен

ВК7	Мейджор 2	5	Екзамен
ВК8	Мейджор 3	5	Екзамен
ВК9	Мейджор 4	5	Екзамен
ВК10	Мейджор 5	5	Екзамен
ВК11	Мейджор 6	5	Екзамен
ВК12	Мейджор 7	5	Екзамен

4.2. ВИБІРКОВА СКЛАДОВА ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Вибіркова складова освітньо-професійної програми складається з:

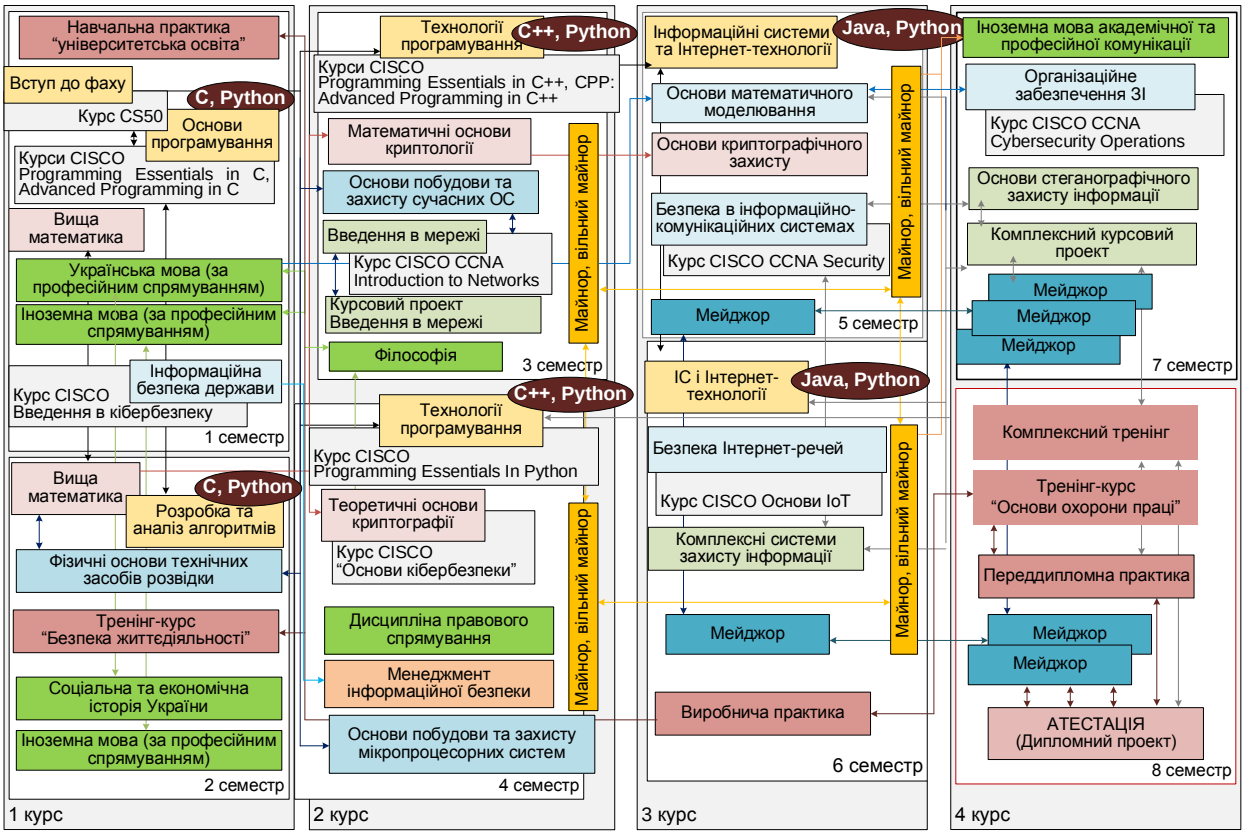
– МАЙНОРІВ – блок взаємопов'язаних непрофільних навчальних дисциплін або ВІЛЬНИЙ МАЙНОР – окремі непрофільні навчальні дисципліни для створення власного МАЙНОРу із загального переліку Університету (загально-університетський пул) для освітньо-кваліфікаційного рівня бакалавр. Дисципліни МАЙНОРІВ є обов'язковими 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 МАЙНОРІВ 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



ПРОЄКТ

V. ФОРМИ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форми атестації здобувачів вищої освіти	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.
Вимоги до кваліфікаційної роботи (дипломного проекту)	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.
Вимоги до публічного захисту (демонстрації за наявності)	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".

Визначення принципів та процедур забезпечення якості вищої освіти	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; 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; забезпечення публічності інформації про освітні програми, 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 напрямами внутрішнього забезпечення якості; зовнішнє оцінювання якості діяльності ХНЕУ ім. С. Кузнеця за результатами участі в національних та міжнародних рейтингах закладів вищої освіти, виконання Ліцензійних вимог, акредитація.
Моніторинг та періодичний перегляд освітніх програм	Моніторинг та періодичний перегляд освітніх програм здійснюється згідно з діючими нормативними актами в ХНЕУ ім. С. Кузнеця: Перегляд освітніх програм здійснюється на основі аналізу задоволеності освітніх потреб виявлених під час моніторингу: - 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. Для перегляду освітніх програм використовуються: онлайн опитування, проведення фокус-групи, аналіз документів, аналіз ситуації, самооцінка робочою групою відповідно вимог до структури та змісту освітньої програми. Періодичність перегляду освітніх програм здійснюється: а) щорічно за результатами моніторингу; б) за завершенням циклу освітньої програми відповідно рівня вищої освіти; в) інші випадки передбачені відповідно до Положення про розроблення, затвердження, моніторинг, періодичний перегляд та оновлення освітніх програм у ХНЕУ ім. С. Кузнеця.
Щорічне оцінювання здобувачів вищої освіти, науково-педагогічних працівників та оприлюднення результатів	Оцінювання здобувачів вищої освіти є послідовним, прозорим та проводиться відповідно до встановлених процедур в Університеті згідно нормативним актам. Щорічне оцінювання здобувачів освіти здійснюється відповідно до: визначеним освітньою програмою формам контролю за встановленими критеріями; порядку оцінювання результатів навчання, що висвітлюється в робочих програмах навчальних дисциплін, робочому плані (технологічній карті) за навчальною дисципліною; обліку результатів навчання, який ведеться з використанням програмного забезпечення корпоративної інформаційної системи управління Університету (електронний журнал) та в електронному курсі з дисципліни на сайті Персональних навчальних систем; 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. Щорічне рейтингове оцінювання діяльності науково-педагогічних працівників, кафедр і факультетів Університету здійснюється за рахунок використання механізмів оцінювання та самооцінювання результативності науково-педагогічної діяльності, її спрямування за пріоритетами розвитку національної системи вищої освіти, стратегій розвитку Університету, особистісними пріоритетами 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
Підвищення кваліфікації	Педагогічні і науково-педагогічні працівники Університету можуть підвищувати кваліфікацію за різними формами, видами

педагогічних, наукових і науково-педагогічних працівників	та у різних суб'єктів підвищення кваліфікації. Забезпечення підвищення кваліфікації відбувається за рахунок: удосконалення раніше набутих та/або набуття нових компетентностей у межах професійної діяльності або галузі знань з урахуванням вимог відповідного професійного стандарту (у разі його наявності); набуття досвіду виконання додаткових завдань та обов'язків у межах спеціальності та/або професії, та/або займаної посади; формування та розвитку цифрової, управлінської, комунікаційної, медійної, інклюзивної, мовленнєвої компетентностей тощо.
Наявність необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за освітньою програмою	Заклад вищої освіти забезпечує освітній процес необхідними та доступними ресурсами (кадровими, методичними, матеріальними, інформаційними та ін.) та здійснюють відповідну підтримку здобувачів вищої освіти. З метою формування практичних та науково-дослідницьких складових компетентностей розгорнуті Кіберполігон та лабораторія блокчейн. При плануванні, розподілі та наданні освітніх ресурсів і забезпеченні підтримки здобувачів вищої освіти враховуються потреби контингенту та принципи студентоцентрованого навчання. Організаційно-методична підтримка самостійної роботи здобувачів вищої освіти, полягає у розробці методичних, дидактичних, інструктивних матеріалів, надає можливість формувати, закріплювати, поглиблювати й систематизувати отримані під час аудиторних занять знання та вміння, здійснювати самопідготовку й самоконтроль опанування освітньої-професійної програми та здійснюється через персональну навчальну систему ХНЕУ ім. С. Кузнеця. Система внутрішнього забезпечення якості освіти гарантує, що всі необхідні ресурси відповідають цілям навчання, є загальнодоступними, а здобувачі вищої освіти поінформовані про їх наявність.
Наявність інформаційних систем для ефективного управління освітнім процесом	З метою управління освітнім процесом розроблено ефективну політику в сфері інформаційного менеджменту та відповідну інтегровану інформаційну система управління освітнім процесом/ корпоративна інформаційна система управління. Дана система передбачає автоматизацію основних функцій управління освітнім процесом, зокрема: забезпечення проведення вступної кампанії, планування та організація освітнього процесу; доступ до освітніх ресурсів; обліку та аналізу успішності здобувачів вищої освіти; адміністрування основних та допоміжних процесів забезпечення освітньої діяльності; управління кадрами та ін.
Публічність інформації про освітні програми, ступені вищої освіти та кваліфікації	Достовірна, об'єктивна, актуальна, своєчасна та легкодоступна інформація за освітньо-професійною програмою "Кібербезпека" публікується на сайті ХНЕУ ім. С. Кузнеця, включаючи програми для потенційних здобувачів вищої освіти, студентів, випускників, інших стейкхолдерів і громадськості. Публічною є інформація про освітню діяльність за

	спеціальністю 125 “Кібербезпека”, освітньо-професійну програму “Кібербезпека”, включаючи критерії відбору на навчання; заплановані результати навчання за цією програмою; процедури навчання, викладання та оцінювання, що використовуються; тощо.
Система запобігання та виявлення академічного плагіату у наукових працях працівників закладів вищої освіти і здобувачів вищої освіти	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, та регулюються 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. Перевірка наукових праць науково-педагогічних працівників Університету та здобувачів вищої освіти щодо дотримання академічної доброчесності 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.

Прийом на освітньо-професійну програму “Кібербезпека” Харківського національного економічного університету імені Семена Кузнеця першого (бакалаврського) рівня вищої освіти здійснюється за результатами вступних випробувань:

1) на основі повної загальної середньої освіти – у формі зовнішнього незалежного оцінювання. У 2021 році приймаються сертифікати зовнішнього незалежного оцінювання 2018 – 2021 років, крім оцінок з англійської, французької, німецької та іспанської мов. Якщо конкурсний предмет обрано іноземну мову, вступник має право подавати оцінку із сертифікатів 2018 – 2021 років з однієї з іноземних мов (англійська, французька, німецька або іспанська) на власний розсуд.

Конкурсні предмети за ОП “Кібербезпека”:

для відкритої конкурсної пропозиції: українська мова та література (К1 = 0,3), математика (К2 = 0,4), іноземна мова або фізика К3 =0,2), вага атестату про повну освіту (К4 = 0,1);

для небюджетних конкурсних пропозицій: українська мова та література (К1 = 0,3), історія України (К2 = 0,3), іноземна мова або географія (К3 = 0,3), вага атестату про повну освіту (К1 = 0,1).

Конкурсний бал обчислюється за формулою:

Конкурсний бал (КБ) = К1*П1 + К2*П2 + К3*П3 + К4*А,

де П1, П2, П3 – оцінки зовнішнього незалежного оцінювання або вступних іспитів з першого, другого та третього предметів; А – середній бал документа про повну загальну середню освіту, переведений в шкалу від 100 до 200 балів відповідно до таблиці переведення середнього балу документа про повну загальну середню освіту, обрахованого за 12-бальною шкалою, в шкалу 100–200.

2) на основі освітньо-кваліфікаційного рівня молодшого спеціаліста – у формі зовнішнього незалежного оцінювання з української мови і літератури, математики та фахового вступного випробування в усній формі. У 2021 році приймаються сертифікати зовнішнього незалежного оцінювання 2018–2021 років.

Конкурсний бал обчислюється за формулою:

Конкурсний бал (КБ) = = К1*П1 + К2*П2 + К3*П3,

де П1, П2 – оцінки зовнішнього незалежного оцінювання з української мови і літератури, та математики. Мінімальна кількість балів, з якими вступник допускається до участі у конкурсі – 100 балів. П3 – оцінка фахового вступного випробування, яке проводиться в усній формі (за шкалою від 100 до 200 балів), мінімальна кількість балів, з якими вступник допускається до участі у конкурсі – 100 балів. К1, К2, К3 – невід'ємні вагові коефіцієнти, українська мова та література (К1 = 0,25), математика (К2 = 0,25), фахове випробування (К3 = 0,5)

Професійні профілі випускників: здатний виконувати професійні роботи (за Державним класифікатором професій ДК 003: 2010):

Код КП	Професійна назва роботи
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
1495	Менеджери (управителі) систем з інформаційної безпеки
2149.2	Фахівець (сфера захисту інформації)
3119	Технік (сфера захисту інформації)
2131.2	Адміністратор бази даних

ПРОЄКТ

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
ЗАГАЛЬНІ КОМПЕТЕНТНОСТІ				
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.		+	+	+
СПЕЦІАЛЬНІ (ФАХОВІ) КОМПЕТЕНТНОСТІ				
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.		+		+

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.	+	+		+
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	+	+		+

ПРОЕКТ

Таблиця 2

Матриця відповідності визначених результатів навчання, компетентностей та освітніх компонентів

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-1	ОК1 ОК4 ОК11 ОК23 ОК29 ОК33 ОК34	ОК6 ОК9 ОК12 ОК13 ОК17 ОК20 ОК25 ОК26 ОК27 ОК31 ОК32 ОК33 ОК34	ОК1 ОК2 ОК30																
РН-2	ОК1 ОК4 ОК11 ОК23 ОК29 ОК33 ОК34	ОК6 ОК9 ОК12 ОК13 ОК17 ОК20 ОК25 ОК26 ОК27 ОК31 ОК32 ОК33 ОК34		ОК11 ОК23 ОК29	ОК4 ОК32 ОК33 ОК34														
РН-3	ОК1 ОК4 ОК11 ОК23 ОК29 ОК33	ОК6 ОК9 ОК12 ОК13 ОК17		ОК11 ОК23 ОК29	ОК4 ОК32 ОК33 ОК34														

ПРОЕКТ

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**
	ОК34	ОК20 ОК25 ОК26 ОК27 ОК31 ОК32 ОК33 ОК34																	
РН-4	ОК1 ОК4 ОК11 ОК23 ОК29 ОК33 ОК34	ОК6 ОК9 ОК12 ОК13 ОК17 ОК20 ОК25 ОК26 ОК27 ОК31 ОК32 ОК33 ОК34		ОК11 ОК23 ОК29	ОК4 ОК32 ОК33 ОК34														
РН-5		ОК6 ОК9 ОК13 ОК17 ОК20 ОК25 ОК26 ОК27 ОК31 ОК32 ОК33 ОК34		ОК11 ОК23 ОК29	ОК4 ОК32 ОК33 ОК34														
РН-6		ОК6 ОК9																	

ПРОЕКТ

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
		ОК13 ОК17 ОК20 ОК25 ОК26 ОК27 ОК31 ОК32 ОК33 ОК34																	
РН-7		ОК6 ОК9 ОК13 ОК17 ОК20 ОК25 ОК26 ОК27 ОК31 ОК32 ОК33 ОК34		ОК11 ОК23 ОК29				ОК9 ОК27 ОК31											
РН-8		ОК6 ОК9 ОК13 ОК17 ОК20 ОК25 ОК26 ОК27 ОК31 ОК32 ОК33 ОК34		ОК11 ОК23 ОК29				ОК9 ОК27 ОК31											

ПРОЕКТ

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-9					ОК4 ОК31 ОК33 ОК34			ОК9 ОК27 ОК31		ОК5 ОК9 ОК13 ОК17 ОК19 ОК20 ОК21 ОК24	ОК6 ОК7 ОК8 ОК20 ОК25 ОК26 ОК27 ОК31	ОК12 ОК13 ОК14 ОК24 ОК34		ОК7 ОК8 ОК10 ОК15 ОК22	ОК34	ОК9 ОК17 ОК20 ОК26 ОК27 ОК28		ОК5 ОК9	ОК8 ОК19 ОК20 ОК21
РН-10	ОК1 ОК4 ОК11 ОК23 ОК29 ОК33 ОК34								ОК8 ОК13 ОК16 ОК18 ОК19 ОК20 ОК22 ОК24 ОК26									ОК5 ОК9	
РН-11	ОК1 ОК4 ОК11 ОК23 ОК29 ОК33 ОК34								ОК8 ОК13 ОК16 ОК18 ОК19 ОК20 ОК22 ОК24 ОК26									ОК5 ОК9	
РН-12														ОК7 ОК8 ОК10 ОК15 ОК22					ОК8 ОК19 ОК20 ОК21
РН-13					ОК4 ОК32 ОК33 ОК34				ОК8 ОК13 ОК16 ОК18			ОК12 ОК13 ОК14 ОК24			ОК34			ОК5 ОК9	ОК8 ОК19 ОК20 ОК21

ПРОЕКТ

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
									ОК19 ОК20 ОК22 ОК24 ОК27			ОК34							
РН-14									ОК8 ОК13 ОК16 ОК18 ОК19 ОК20 ОК22 ОК24 ОК26	ОК5 ОК9 ОК13 ОК17 ОК19 ОК20 ОК21 ОК22		ОК12 ОК13 ОК14 ОК24 ОК34			ОК34		ОК32 ОК33	ОК5 ОК9	
РН-15									ОК8 ОК13 ОК16 ОК18 ОК19 ОК20 ОК22 ОК24 ОК26	ОК5 ОК9 ОК13 ОК17 ОК19 ОК20 ОК21 ОК24								ОК5 ОК9	
РН-16								ОК9 ОК27 ОК31		ОК5 ОК9 ОК13 ОК17 ОК19 ОК20 ОК21 ОК24				ОК7 ОК8 ОК10 ОК15 ОК22					ОК8 ОК19 ОК20 ОК21
РН-17		ОК6 ОК9 ОК13 ОК17							ОК8 ОК13 ОК16 ОК18	ОК5 ОК9 ОК13 ОК17	ОК6 ОК7 ОК8 ОК20	ОК12 ОК13 ОК14 ОК24	ОК15 ОК16 ОК19 ОК20		ОК34			ОК5 ОК9	

ПРОЕКТ

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
		ОК20 ОК25 ОК26 ОК27 ОК31 ОК32 ОК33 ОК34							ОК19 ОК20 ОК22 ОК24 ОК26	ОК19 ОК20 ОК21 ОК24	ОК25 ОК26 ОК27 ОК31	ОК34	ОК26 ОК34						
РН-18	ОК1 ОК4 ОК11 ОК23 ОК29 ОК33 ОК34								ОК8 ОК13 ОК16 ОК18 ОК19 ОК20 ОК22 ОК24 ОК26	ОК5 ОК9 ОК13 ОК17 ОК19 ОК20 ОК21 ОК24		ОК12 ОК13 ОК14 ОК24 ОК34						ОК5 ОК9	
РН-19	ОК1 ОК4 ОК11 ОК23 ОК29 ОК33 ОК34								ОК8 ОК12 ОК13 ОК16 ОК18 ОК19 ОК20 ОК22 ОК24 ОК26			ОК12 ОК13 ОК14 ОК24 ОК34			ОК34			ОК5 ОК9	
РН-20	ОК1 ОК4 ОК11 ОК23 ОК29 ОК33 ОК34								ОК8 ОК12 ОК13 ОК16 ОК18 ОК19 ОК20	ОК5 ОК9 ОК12 ОК13 ОК17 ОК19 ОК20		ОК12 ОК13 ОК14 ОК24 ОК34	ОК15 ОК16 ОК19 ОК20 ОК26 ОК34				ОК32 ОК33		

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
									ОК22 ОК24 ОК26	ОК21 ОК24									
РН-21	ОК1 ОК4 ОК11 ОК23 ОК29 ОК33 ОК34											ОК12 ОК13 ОК14 ОК24 ОК34				ОК9 ОК17 ОК20 ОК26 ОК27 ОК28		ОК5 ОК9	
РН-22	ОК1 ОК4 ОК11 ОК23 ОК29 ОК33 ОК34											ОК12 ОК13 ОК14 ОК24 ОК34						ОК5 ОК9	
РН-23												ОК12 ОК13 ОК14 ОК24 ОК34	ОК15 ОК16 ОК19 ОК20 ОК26 ОК34		ОК34			ОК5 ОК9	
РН-24	ОК1 ОК4 ОК11 ОК23 ОК29 ОК33 ОК34										ОК6 ОК7 ОК8 ОК20 ОК25 ОК26 ОК27 ОК31	ОК12 ОК13 ОК14 ОК24 ОК34				ОК9 ОК17 ОК20 ОК26 ОК27 ОК28		ОК5 ОК9	
РН-25												ОК12 ОК13			ОК34	ОК9 ОК17		ОК5 ОК9	

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
												ОК14 ОК24 ОК34				ОК20 ОК26 ОК27 ОК28			
РН-26												ОК12 ОК13 ОК14 ОК24 ОК34						ОК5 ОК9	
РН-27	ОК1 ОК4 ОК11 ОК23 ОК29 ОК33 ОК34										ОК6 ОК7 ОК8 ОК20 ОК25 ОК26 ОК27 ОК31	ОК12 ОК13 ОК14 ОК24 ОК34	ОК15 ОК16 ОК19 ОК20 ОК26 ОК34						
РН-28					ОК4 ОК32 ОК33 ОК34							ОК12 ОК13 ОК14 ОК24 ОК34				ОК9 ОК17 ОК20 ОК26 ОК27 ОК28			ОК8 ОК19 ОК20 ОК21
РН-29										ОК5 ОК9 ОК13 ОК17 ОК19 ОК20 ОК21 ОК24 ОК26	ОК6 ОК7 ОК8 ОК20 ОК25 ОК26 ОК27 ОК31	ОК12 ОК13 ОК14 ОК24 ОК34			ОК34	ОК9 ОК17 ОК20 ОК26 ОК27 ОК28			ОК8 ОК19 ОК20 ОК21
РН-30																			ОК8 ОК19

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
																			ОК20 ОК21
РН-31									ОК8 ОК12 ОК13 ОК16 ОК18 ОК19 ОК20 ОК22 ОК24 ОК27				ОК15 ОК16 ОК19 ОК20 ОК26 ОК34				ОК32 ОК33		
РН-32	ОК1 ОК4 ОК11 ОК23 ОК29 ОК33 ОК34										ОК6 ОК7 ОК8 ОК20 ОК25 ОК26 ОК27 ОК31	ОК12 ОК13 ОК14 ОК24 ОК34			ОК34			ОК5 ОК9	
РН-33								ОК9 ОК27 ОК31			ОК6 ОК7 ОК8 ОК20 ОК25 ОК26 ОК27 ОК31				ОК34	ОК9 ОК17 ОК20 ОК26 ОК27 ОК28			ОК8 ОК19 ОК20 ОК21
РН-34								ОК9 ОК27 ОК31			ОК6 ОК7 ОК8 ОК20 ОК25 ОК26 ОК27	ОК12 ОК13 ОК14 ОК24 ОК34			ОК34	ОК9 ОК17 ОК20 ОК26 ОК27 ОК28			ОК8 ОК19 ОК20 ОК21

ПРОЕКТ

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
											ОК31								
РН-35	ОК1 ОК4 ОК11 ОК23 ОК29 ОК33 ОК34							ОК9 ОК27 ОК31		ОК5 ОК9 ОК12 ОК13 ОК17 ОК19 ОК20 ОК21 ОК24	ОК6 ОК7 ОК8 ОК20 ОК25 ОК26 ОК27 ОК31	ОК12 ОК13 ОК14 ОК24 ОК34		ОК7 ОК8 ОК10 ОК15 ОК22	ОК34	ОК9 ОК17 ОК20 ОК26 ОК27 ОК28			ОК8 ОК19 ОК20 ОК21
РН-36																	ОК32 ОК33		
РН-37													ОК15 ОК16 ОК19 ОК20 ОК26 ОК34				ОК32 ОК33		
РН-38													ОК15 ОК16 ОК19 ОК20 ОК26 ОК34				ОК32 ОК33		
РН-39																	ОК32 ОК33		
РН-40																	ОК32 ОК33		
РН-41									ОК22						ОК34			ОК5 ОК9	
РН-42											ОК6 ОК7 ОК8 ОК20 ОК25	ОК12 ОК13 ОК14 ОК24 ОК34			ОК34	ОК9 ОК17 ОК20 ОК26 ОК27		ОК5 ОК9	ОК8 ОК19 ОК20 ОК21

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
											ОК26 ОК27 ОК31					ОК28			
РН-43		ОК6 ОК9 ОК12 ОК13 ОК17 ОК20 ОК25 ОК26 ОК27 ОК31 ОК32 ОК33 ОК34						ОК9 ОК27 ОК31			ОК6 ОК7 ОК8 ОК20 ОК25 ОК26 ОК27 ОК31	ОК12 ОК13 ОК14 ОК24 ОК34			ОК34	ОК9 ОК17 ОК20 ОК26 ОК27 ОК28		ОК5 ОК9	ОК8 ОК19 ОК20 ОК21
РН-44								ОК9 ОК27 ОК31			ОК6 ОК7 ОК8 ОК20 ОК25 ОК26 ОК27 ОК31	ОК12 ОК13 ОК14 ОК24 ОК34			ОК34	ОК9 ОК17 ОК20 ОК26 ОК27 ОК28		ОК5 ОК9	ОК8 ОК19 ОК20 ОК21
РН-45											ОК6 ОК7 ОК8 ОК20 ОК25 ОК26 ОК27 ОК31	ОК12 ОК13 ОК14 ОК24 ОК34			ОК34	ОК9 ОК17 ОК20 ОК26 ОК27 ОК28			ОК8 ОК19 ОК20 ОК21
РН-46											ОК6 ОК7	ОК12 ОК13			ОК34	ОК9 ОК17			ОК8 ОК19

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
											ОК8 ОК20 ОК25 ОК26 ОК27 ОК31	ОК14 ОК24 ОК34				ОК20 ОК26 ОК27 ОК28			ОК20 ОК21
РН-47									ОК8 ОК12 ОК13 ОК16 ОК18 ОК19 ОК20 ОК24 ОК26	ОК5 ОК9 ОК12 ОК13 ОК17 ОК19 ОК20 ОК21 ОК24		ОК12 ОК13 ОК14 ОК24 ОК34					ОК32 ОК33		
РН-48												ОК12 ОК13 ОК14 ОК24 ОК34	ОК15 ОК16 ОК19 ОК20 ОК26 ОК34		ОК34		ОК32 ОК33	ОК5 ОК9	
РН-49												ОК12 ОК13 ОК14 ОК24 ОК34	ОК15 ОК16 ОК19 ОК20 ОК26 ОК34		ОК34			ОК5 ОК9	
РН-50										ОК5 ОК9 ОК12 ОК13 ОК17 ОК19 ОК20 ОК21		ОК12 ОК13 ОК14 ОК24 ОК34			ОК34			ОК5 ОК9	

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
										ОК24									
РН-51												ОК12 ОК13 ОК14 ОК24 ОК34			ОК34			ОК5 ОК9	
РН-52												ОК12 ОК13 ОК14 ОК24 ОК34	ОК15 ОК16 ОК19 ОК20 ОК26 ОК34		ОК34			ОК5 ОК9	
РН-53	ОК1 ОК4 ОК11 ОК23 ОК29 ОК33 ОК34			ОК11 ОК23 ОК29					ОК8 ОК12 ОК13 ОК16 ОК18 ОК19 ОК20 ОК22 ОК24 ОК25	ОК5 ОК9 ОК12 ОК13 ОК17 ОК19 ОК20 ОК21 ОК22	ОК6 ОК7 ОК8 ОК20 ОК25 ОК26 ОК27 ОК31	ОК12 ОК13 ОК14 ОК24 ОК34	ОК15 ОК16 ОК19 ОК20 ОК26 ОК34		ОК34			ОК5 ОК9	ОК8 ОК19 ОК20 ОК21
РН-54	ОК1 ОК4 ОК11 ОК23 ОК29 ОК33 ОК34	ОК6 ОК9 ОК12 ОК13 ОК17 ОК20 ОК25 ОК26 ОК27				ОК3 ОК4 ОК11 ОК23 ОК29 ОК32 ОК34	ОК3 ОК11 ОК29 ОК34												

ПРОЕКТ

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
		ОК31 ОК32 ОК33 ОК34																	

Гарант ОП **_____** **Євсеєв С.П.**
завідувач кафедри кібербезпеки
та інформаційних технологій, д.т.н., проф.

ПРОЕКТ