ПРОЕКТ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ЗАТВЕРДЖЕНО
Вченою радою ХНЕУ ім. С. Кузнеця
Протокол № ___ від _____ р.
Голова Вченої ради
Ректор _____ В. С. Пономаренко

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА КІБЕРБЕЗПЕКА / CYBERSECURITY

РІВЕНЬ ВИЩОЇ ОСВІТИ	**перший (бакалаврський)**
СТУПІНЬ ВИЩОЇ ОСВІТИ	**бакалавр**
ГАЛУЗЬ ЗНАНЬ	**12 Інформаційні технології**
СПЕЦІАЛЬНІСТЬ	**125 Кібербезпека (CYBERSECURITY)**

ХАРКІВ, 2020

І. Преамбула

1. ЗАТВЕРДЖЕНО ТА НАДАНО ЧИННОСТІ

Освітньо-професійна програма вищої освіти галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека забезпечення першого (бакалаврського) рівня вищої освіти затверджена та введена в дію Наказом ректора Харківського національного економічного університету імені Семена Кузнеця від _____ р. № ___ у відповідності до рішення вченої ради університету від _____ р. Протокол № ___, розглянуто на засіданні кафедри кібербезпеки та інформаційних технологій 27.02.2020 р. Протокол № 11.

2. РОЗРОБНИКИ ОПП

Євсеєв Сергій Петрович, доктор технічних наук, завідувач кафедри кібербезпеки та інформаційних технологій.

Алексієв Володимир Олегович, доктор технічних наук, професор кафедри кібербезпеки та інформаційних технологій.

Мілов Олександр Володимирович, кандидат технічних наук, професор кафедри кібербезпеки та інформаційних технологій.

Ковтун Владислав Юрійович, кандидат технічних наук, технічний директор ТОВ “Сайфер БІС”.

Кравченко Павло Олександрович, співзасновник “Distributed Lab”.

Макаренко Антон Олегович, студент 4 курсу першого (бакалаврського) рівня вищої освіти за спеціальністю 125 “Кібербезпека”.

ІІ. Загальна характеристика

Рівень вищої освіти	Перший (бакалаврський) рівень FQ-EHEA – перший цикл, EQF LLL – 6 рівень, НРК – 7 рівень / Бакалавр
Ступінь вищої освіти	Бакалавр
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня кваліфікація	Бакалавр з кібербезпеки
Професійна(і) кваліфікація(ї) (тільки для регульованих професій)	–
Опис предметної області	*Об'єкти професійної діяльності випускників*: – 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

<table>
<tr><td></td><td>технології забезпечення інформаційної та/ або кібербезпеки.
Інструменти та обладнання:
– системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки;
– сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.</td></tr>
<tr><td>Академічні права випускників</td><td>Можливість продовжити навчання за освітньою програмою ступеня магістра</td></tr>
<tr><td>Працевлаштування випускників (тільки для регульованих професій)</td><td>
<table>
<tr><th>КОД КП</th><th>КОД ЗКППТР</th><th>ВИПУСК ДКХП</th><th>Професійна назва роботи</th></tr>
<tr><td>3439</td><td>24771</td><td></td><td>Фахівець із організації інформаційної безпеки</td></tr>
<tr><td colspan="4">International Standard Classification of Occupations 2008 (ISCO-08)</td></tr>
<tr><td>Code</td><td></td><td></td><td>Occupation</td></tr>
<tr><td>2529</td><td></td><td></td><td>Security specialist (ICT)</td></tr>
</table>
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.</td></tr>
</table>

ІІІ. Обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти

Обсяг освітньої програми підготовки бакалавра галузі знань 12 Інформаційні технології спеціальності 125 “Кібербезпека”:

на базі повної загальної середньої освіти з терміном навчання 11 років – 240 кредитів ЄКТС;

на базі повної загальної середньої освіти з терміном навчання 12 років – 240 кредитів ЄКТС.

Термін навчання: денна форма – 3 роки 10 місяців; заочна форма – 4 роки 10 місяців.

Обсяг освітньої програми підготовки бакалавра галузі знань 12 Інформаційні технології, спеціальність 125 Кібербезпека ступеня молодшого спеціаліста:

на базі освітнього ступеня молодшого спеціаліста (бакалавра) спорідненої спеціальності – 240 кредитів ЄКТС;

на базі освітнього ступеня молодшого спеціаліста (бакалавра) інших спеціальностей – 240 кредитів ЄКТС.

Термін навчання: денна форма – 2 роки 10 місяців для споріднених спеціальностей (2 роки 10 місяців – для інших спеціальностей); заочна форма – 2 роки 10 місяців для всіх спеціальностей.

Обсяг кредитів ЄКТС для здобуття ступеня бакалавра зі спеціальності 125 Кібербезпека

Цикли підготовки	Кількість кредитів ECTS
Освітня програма бакалавра за циклами на базі повної загальної середньої освіти:	**240**
Цикл загальної підготовки	**29 (12 %)**
Цикл професійної підготовки	**211 (88 %)**

IV. 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.

Фахові компетентності	КФ 1. Здатність застосовувати законодавчу та нормативноправову 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.
	К 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.

V. Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання

№	Результати навчання
РН–1	застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
РН–2	організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих 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

№	Результати навчання
	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

№	Результати навчання
	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

№	Результати навчання
	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.

Загальні компетентності	Результати навчання
КЗ 1. Здатність застосовувати знання у практичних ситуаціях.	РН–1, РН–2, РН–3, РН–4, РН–10, РН–11, РН–18, РН–21, РН–22, РН–24, 27 РН–32, РН–35 РН–54
КЗ 2. Знання та розуміння предметної області та розуміння професії.	РН–1, РН–2, РН–3, РН–4, РН–5, РН–6, РН–7, РН–8, РН–17, РН–43, РН–54
КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово	РН–1
КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням	РН–2, РН–3, РН–4, РН–5, РН–7, РН–8
КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.	РН–2, РН–3, РН–4, РН–5, РН–9, РН–13, РН–28
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	РН–54

Загальні компетентності	Результати навчання
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.	РН–54
Фахові компетентності	Результати навчання
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.	РН–7, РН–8, РН–9, РН–16, РН–33, РН–34, РН–35, РН–43, РН–44
КФ 2. Здатність до використання інформаційно комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.	РН–10, РН–11, РН–13, РН–14, РН–15, РН–17, РН–18, РН–19, РН–20, РН–31, РН–47
КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.	РН–9, РН–14, РН–15, РН–16, РН–17, РН–18, РН–20, РН–29, РН–35, РН–47, РН–50
КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.	РН–9, РН–17, РН–24, РН–27, РН–29, РН–32, РН–33, РН–34, РН–35, РН–42, РН–43, РН–44, РН–45, РН–46
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	РН–9, РН–13, РН–14, РН–17, РН–18, РН–19, РН–20, РН–21, РН–22, РН–23, РН–24, РН–25, РН–26, РН–27, РН–28, РН–29, РН–32, РН–34, РН–35, РН–42, РН–43, РН–44, РН–45, РН–46, РН–47, РН–48, РН–49, РН–50, РН–51, РН–52
КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.	РН–17, РН–20, РН–23, РН–27, РН–31, РН–37, РН–38, РН–48, РН–49, РН–52
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.)	РН–9, РН–12, РН–16, РН–35
КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.	РН–9, РН–13, РН–14, РН–17, РН–19, РН–23, РН–25, РН–29, РН–32, РН–33, РН–34, РН–35, РН–41, РН–42, РН–43, РН–44, РН–45, РН–46, РН–48, РН–49, РН–50, РН–51, РН–52

Загальні компетентності	Результати навчання
КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.	РН–9, РН–21, РН–24, РН–25, РН–28, РН–29, РН–33, РН–34, РН–35, РН–42, РН–43, РН–44, РН–45, РН–46
КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.	РН–14, РН–20, РН–31, РН–36, РН–37, РН–38, РН–39, РН–40, РН–47, РН–48
КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН–9, РН–10, 11, РН–13, РН–14, РН–15, РН–17, РН–18, РН–19, РН–21, РН–22, РН–23, РН–24, РН–25, РН–26, РН–32, РН–41, РН–42, РН–43, РН–48, РН–49, РН–50, РН–51, РН–52
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.	РН–9, РН–12, РН–13, РН–16, РН–28, РН–29, РН–30, РН–33, РН–34, РН–35, РН–42, РН–43, РН–44, РН–45, РН–46

СТРУКТУРА ПРОГРАМИ ПІДГОТОВКИ БАКАЛАВРІВ

Галузь знань 12 “Інформаційні технології”,
спеціальність 125 “Кібербезпека”

Складові освітньо-професійної програми	Загальна кількість		Структура, %
	кредитів ЄКТС	годин	
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ	**29**	**870**	**12%**
БАЗОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ	*24*	*720*	*10%*
ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ	*5*	*150*	*2%*
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ	**211**	**6330**	**88%**
БАЗОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ	*155*	*4650*	*65%*
ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ	*56*	*1680*	*23%*
ЗАГАЛЬНА КІЛЬКІСТЬ :	**240**	**7200**	**100%**
в тому числі: вибіркова складова	*61*	*1830*	*25%*

Шифр дисципліни	Складові освітньо-професійної програми	Загальна кількість		Форма контролю
		кредитів ЄКТС	годин	
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ				
БАЗОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ				
ЗЦ 1.1	Українська мова (за професійним спрямуванням)	5	150	Екзамен
ЗЦ 1.2	Іноземна мова (за професійним спрямуванням)	9	270	Залік, Екзамен
ЗЦ 1.3	Соціальна та економічна історія України	5	150	Екзамен
ЗЦ 1.4	Філософія	5	150	Екзамен
РАЗОМ БАЗОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ:		**24**	**720**	
ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ (Вибір навчальних дисциплін здійснюється із загальноуніверситетського пулу)				
ЗЦ 2.1	Дисципліна правового спрямування	5	150	Екзамен
РАЗОМ ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ:		**5**	**150**	
РАЗОМ ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ		**29**	**870**	

ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ				
БАЗОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ				
ПЦ 1	Вища математика	15	450	Залік, Екзамен
ПЦ 2	Вступ до фаху	4	120	Залік
ПЦ 3	Розробка та аналіз алгоритмів	5	150	Екзамен
ПЦ 4	Фізичні основи технічних засобів розвідки	4	120	Залік
ПЦ 5	Інформаційна безпека держави	5	150	Залік
ПЦ 6	Основи програмування	5	150	Екзамен
ПЦ 7	Навчальна практика "університетська освіта"	1	30	Залік
ПЦ 8	Тренінг-курс «безпека життєдіяльності»	2	60	Залік
ПЦ 9	Математичні основи криптології	4	120	Залік
ПЦ 10	Теоретичні основи криптографії	5	150	Екзамен
ПЦ 11	Основи побудови та захисту сучасних операційних систем	5	150	Екзамен
ПЦ 12	Технології програмування	12	360	Залік, Екзамен
ПЦ 13	Основи побудови та захисту мікропроцесорних систем	4	120	Залік
ПЦ 14	Менеджмент інформаційної безпеки	4	120	Залік
ПЦ 15	Курсовий проект: введення в мережі	1	30	КП
ПЦ 16	Введення в мережі	5	150	Екзамен
ПЦ 17	Інформаційні системи та інтернет технології	11	330	Залік, Екзамен
ПЦ 18	Основи математичного моделювання	4	120	Залік
ПЦ 19	Організація та інформаційне забезпечення управлінської діяльності	5	150	Екзамен
ПЦ 20	Виробнича практика	4	120	ЗВІТ
ПЦ 21	Основи криптографічного захисту	4	120	Залік
ПЦ 22	Комплексні системи захисту інформації	5	150	Залік
ПЦ 23	Безпека в інформаційно-комунікаційних системах	5	150	Екзамен
ПЦ 24	Комплексний курсовий проект	1	30	КП
ПЦ 25	Основи стеганографічного захисту інформації	5	150	Екзамен
ПЦ 26	Тренінг-курс «основи охорони праці»	2	60	Залік
ПЦ 27	Іноземна мова академічної та професійної комунікації	5	150	Залік
ПЦ 28	Організаційне забезпечення захисту інформації	5	150	Екзамен
ПЦ 29	Комплексний тренінг	3	90	ЗВІТ
ПЦ 30	Переддипломна практика	5	150	ЗВІТ

ПЦ 31	Дипломний проект	10	300	Дипломний проект
РАЗОМ БАЗОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ:		**154**	**4620**	
ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ				
	(Студенти обирають 4 навчальні дисципліни із загальноуніверситетського пулу)			
МНР 1	Майнор або вільний майнор	5	150	Залік
МНР 2	Майнор або вільний майнор	5	150	Залік
МНР 3	Майнор або вільний майнор	5	150	Залік
МНР 4	Майнор або вільний майнор	5	150	Залік
ВСЬОГО МАЙНОР:		**20**	**600**	
(Студенти обирають один із запропонованих мейджорів) **МЕЙДЖОР "ЗАХИСТ КОРПОРАТИВНИХ МЕРЕЖ"**				
МДР 1.1	Корпоративні мережі та системи доступу	7	210	Екзамен
МДР 1.2	Безпека та аудит бездротових та рухомих мереж	5	150	Екзамен
МДР 1.3	Основи планування та адміністрування служб доступу до інформаційних ресурсів	4	120	Залік
МДР 1.4	Адміністрування Unix-подібних систем	5	150	Залік
МДР 1.5	Мережне програмування	5	150	Екзамен
МДР 1.6	Основи технічного захисту інформації	5	150	Екзамен
МДР 1.7	Експертні системи	5	150	Екзамен
МЕЙДЖОР "БЛОКЧЕЙН-ТЕХНОЛОГІЯ ТА БЕЗПЕКА БАНКІВСЬКИХ СИСТЕМ"				
МДР 2.1	Blockchain: основи та приклади застосування	5	150	Екзамен
МДР 2.2	Основи смарт-контрактів	4	120	Залік
МДР 2.3	Основи розробки децентралізованих застосувань (decentralized applications (dapps))	5	150	Залік
МДР 2.4	Безпека банківських систем	5	150	Екзамен
МДР 2.5	Безпека в Devops	5	150	Екзамен
МДР 2.6	Основи технічного захисту інформації	5	150	Екзамен
МДР 2.7	Організація і збереження баз даних	7	210	Екзамен
ВСЬОГО ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ (МАЙНОРИ, МЕЙДЖОРИ)		**56**	**1680**	
ВСЬОГО ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ		**211**	**6330**	
ЗАГАЛЬНА КІЛЬКІСТЬ		**240**	**7200**	

VI. Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація за спеціальністю 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. Результати атестації визначаються оцінками за національною шкалою: “відмінно”, “добре”, “задовільно”, “незадовільно”.
Вимоги до заключної кваліфікаційної роботи (за наявності)	Харківський національний економічний університет імені Семена Кузнеця розробляє та затверджує: 1) Положення про атестацію випускників Харківського національного економічного університету імені Семена Кузнеця; 2) Порядок перевірки кваліфікаційних робіт бакалаврів на плагіат. Атестація осіб, які здобувають ступінь бакалавра, здійснюється ЕК, до складу якої можуть включатися відомі фахівці у галузі кібербезпеки та представники роботодавців. Кваліфікаційна дипломна робота бакалавра допускається до захисту перед ЕК за умови, якщо рівень її унікальності (оригінальності) відповідає нормативу, який затверджений рішенням кафедри кібербезпеки та інформаційних технологій Харківського національного економічного університету імені Семена Кузнеця. Вимоги до заключної кваліфікаційної роботи: Кваліфікаційний проект (кваліфікаційна робота) має передбачати розв’язання складного спеціалізованого завдання або практичної проблеми в галузі кібербезпеки, що характеризується комплексністю та невизначеністю умов, із застосуванням теорій та методів кібербезпеки та демонструвати вміння автора використовувати надбані компетентності та результати навчання, логічно, на підставі сучасних наукових методів викладати та обґрунтовувати свої погляди за темою дослідження, робити відповідні висновки і формулювати конкретні пропозиції та рекомендації щодо результатів розв’язаних завдань, а також показувати схильність автора до наукової або практичної діяльності у сфері кібербезпеки.
	Для оприлюднення та публічного ознайомлення зі змістом кваліфікаційних проектів, запобігання академічного плагіату дипломні проекти мають бути розміщені на офіційному сайті Харківського національного економічного університету імені Семена Кузнеця.

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 студента повинна супроводжуватися презентаційними матеріалами та пояснювальною запискою, призначеними для загального перегляду. Ухвалення екзаменаційною комісією рішення про присудження ступеня бакалавра з кібербезпеки та видачу диплома бакалавра за результатами підсумкової атестації студентів оголошуються після оформлення в установленому порядку протоколів засідань екзаменаційної комісії.

VII. 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”.

Принципи та процедури забезпечення якості освіти	**Принципи забезпечення якості освіти:** • відповідальність за якість вищої освіти, що надається; • забезпечення якості відповідає різноманітності систем вищої освіти, закладів вищої освіти, програм і студентів; забезпечення якості сприяє розвитку культури якості; • забезпечення якості враховує потреби та очікування студентів, усіх громадян та суспільства в цілому. **Процедурами забезпечення якості освіти є:** • розроблення та впровадження стратегії і політики в сфері якості вищої освіти; • розроблення механізму формування, затвердження, моніторингу та поточного перегляду змісту освітніх програм;
	• розроблення та впровадження системи оцінювання знань здобувачів вищої освіти, науково-педагогічних і педагогічних працівників та регулярного оприлюднення результатів таких оцінювань на офіційному веб-сайті ХНЕУ ім. С. Кузнеця, на інформаційних стендах та в будь-який інший спосіб, згідно з розробленими та затвердженими правилами; • організація постійного підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників; • формування необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за кожною освітньою програмою; • створення та функціонування інформаційних систем для ефективного управління якістю освітнього процесу; • оприлюднення об’єктивної неупередженої інформації про освітні програми, ступені вищої освіти та кваліфікації; • розроблення політик щодо ефективної системи запобігання та виявлення академічного плагіату у наукових працях здобувачів вищої освіти; • інших процедур і заходів.

Моніторинг та періодичний перегляд освітніх програм	Моніторинг і періодичний перегляд програм здійснюється з метою забезпечення їх відповідності потребам студентів і суспільства. Моніторинг спрямований на безперервне вдосконалення програм. Регулярний моніторинг, перегляд і оновлення освітніх програм мають гарантувати відповідний рівень надання освітніх послуг, а також створює сприятливе й ефективне навчальне середовище для здобувачів вищої освіти. Це передбачає оцінювання: • змісту програми в контексті останніх досліджень у сфері кібербезпеки, гарантуючи відповідність програм сучасним вимогам; • рівня навчального навантаження здобувачів вищої освіти, їх досягнень і результатів завершення освітньої програми; • ефективності процедур оцінювання студентів; • очікувань, потреб і задоволеності здобувачів вищої освіти змістом та процесом навчання; • забезпечення якості сервісних послуг для здобувачів вищої освіти. Програми регулярно переглядаються та оновлюються із залученням до цього процесу здобувачів вищої освіти, фахівців
Щорічне оцінювання здобувачів вищої освіти	Оцінювання здобувачів вищої освіти базується на принципах студентоцентрованого навчання та передбачає наступне: • оцінювачі (експерти) ознайомлені з існуючими методами проведення тестування та екзаменування і отримують підтримку для розвитку власних навичок у цій сфері; • критерії та методи оцінювання, а також критерії виставлення оцінок оприлюднюються заздалегідь; • оцінювання здобувачів вищої освіти дозволяє продемонструвати ступінь досягнення ними запланованих результатів навчання; • оцінювання проводиться предметною комісією у складі більше ніж дві особи; • процедури оцінювання здобувачів вищої освіти повинні враховувати пом'якшувальні обставини; • оцінювання здобувачів вищої освіти є послідовним, прозорим та проводиться відповідно до встановлених процедур; • наявність офіційної процедури розгляду апеляцій здобувачів вищої освіти.
Підвищення кваліфікації науково-педагогічних, педагогічних та наукових працівників	Система підвищення кваліфікації науково-педагогічних, педагогічних та наукових працівників розробляється у відповідності до діючої нормативної бази та будується на наступних принципах: • обов'язковості та періодичності проходження стажування і підвищення кваліфікації; • прозорості процедур організації стажування та підвищення кваліфікації; • моніторингу відповідності змісту програм підвищення кваліфікації задачам професійного діяльності; обов'язковості впровадження результатів підвищення кваліфікації в наукову та педагогічну діяльність; • оприлюднення отриманих результатів стажування та підвищення кваліфікації.

Наявність необхідних ресурсів для організації освітнього процесу	Вищі навчальні заклади забезпечують освітній процес необхідними та доступними для здобувачів вищої освіти ресурсами (кадровими, методичними, матеріальними, інформаційними та ін.) та здійснюють відповідну підтримку студентів. При плануванні, розподілі та наданні навчальних ресурсів і забезпеченні підтримки здобувачів вищої освіти враховуються потреби різноманітного студентського контингенту (такого як студенти: з досвідом, заочної форми навчання, що працюють, іноземні студенти, студентів з особливими потребами). Внутрішнє забезпечення якості освіти гарантує, що всі необхідні ресурси відповідають цілям навчання, є загальнодоступними, а студенти поінформовані про їх наявність та можуть їх використовувати у навчанні.
Наявність інформаційних систем для ефективного управління освітнім процесом	З метою управління освітніми процесами розроблено ефективну політику та відповідну інтегровану інформаційну система управління освітнім процесом. Дана система передбачає автоматизацію основних функцій управління освітнім процесом, зокрема: автоматизоване забезпечення проведення вступної компанії, використання сучасник інформаційних технологій для планування та організації навчального процесу; доступ до навчальних ресурсів на сайті університету; облік та аналіз успішності здобувачів вищої освіти; адміністрування основних та допоміжних процесів забезпечення освітньої діяльності; моніторинг дотримання стандартів якості; управління кадровим забезпеченням тощо.
Публічність інформації про освітні програми, ступені вищої освіти та кваліфікації	Достовірна, об’єктивна, актуальна та легкодоступна інформація про навчальний процес за спеціальністю 125 Кібербезпека публікується на сайті ХНЕУ ім. С. Кузнеця, включаючи програми для потенційних здобувачів вищої освіти, студентів, випускників, громадськості, включаючи: програми, критерії відбору на навчання; заплановані результати навчання за цими програмами; кваліфікації; процедури навчання, викладання та оцінювання, що використовуються; прохідні бали та навчальні можливості, доступні для студентів, тощо.
Запобігання та виявлення академічного плагіату у наукових працях працівників вищих навчальних закладів і здобувачів вищої освіти;	Система забезпечення академічної доброчесності учасниками освітнього процесу в ХНЕУ ім. С. Кузнеця, базується на таких принципах: • дотримання загальноприйнятих принципів моралі та наукової етики; • повага до Конституції і законів України і дотримання їхніх норм; • повага до всіх учасників освітнього процесу незалежно від їхнього світогляду, соціального стану, релігійної та національної приналежності; • дотримання норм чинного законодавства про авторське право; • посилання на джерела інформації у разі запозичень ідей, тверджень, відомостей; У випадку порушення принципів наукової та освітянської доброчесності та моральних принципів відповідні особи притягуються до відповідальності відповідно до чинного законодавства України та діючих у ХНЕУ ім. С. Кузнеця положень та норм.

VIII. Перелік нормативних документів, на яких базується освітньо-професійна програма

Згідно зі статтею 32 п. 1 Закону України "Про вищу освіту" Харківський національний економічний університет імені Семена Кузнеця проводить підготовку бакалаврів за спеціальністю 125 Кібербезпека.

Діяльність вищого навчального закладу провадиться на принципах:

1) автономії та самоврядування;

2) розмежування прав, повноважень і відповідальності засновника (засновників), державних органів та органів місцевого самоврядування, до сфери управління яких належить вищий навчальний заклад, органів управління вищого навчального закладу та його структурних підрозділів;

3) поєднання колегіальних та єдиноначальних засад;

4) незалежності від політичних партій, громадських і релігійних організацій (крім вищих духовних навчальних закладів).

Перелік використаних джерел

1. TUNING (для ознайомлення зі спеціальними (фаховими) компетентностями та прикладами стандартів – http://www.unideusto.org/tuningeu/.
2. Закон «Про вищу освіту» [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1556-18.
3. Національний глосарій 2014 [Електронний ресурс]. – Режим доступу: http://ihed.org.ua/images/biblioteka /glossariy_Visha_osvita_2014_tempus-office.pdf.
4. Національний класифікатор України: "Класифікатор професій" ДК 003:2010 // [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/rada/show/va327609-10
5. Постанова Кабінету Міністрів України від 23.11.11 р. № 1341 «Про затвердження Національної рамки кваліфікацій. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1341-2011-п.
6. Постанова Кабінету Міністрів України від 29.04.15 р. № 266 "Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти". [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/266-2015-п.

7. Постанова Кабінету Міністрів №1187 “Про затвердження ліцензійних умов провадження освітньої діяльності закладів освіти” від 30.12.2015 р.

8. Наказ МОН України №166 “Деякі питання оприлюднення інформації про діяльність вищих навчальних закладів” від 19.02.2015 р.

9. Рашкевич Ю.М. Болонський процес та нова парадигма вищої освіти: Монографія. – Львів : Видавництво Львівської політехніки. – 2014. – 168 с.

10. Розвиток системи забезпечення якості вищої освіти в Україні: інформаційно-аналітичний огляд [Електронний ресурс]. – Режим доступу: http://ihed.org.ua/images/biblioteka /Rozvitok_sisitemi_zabesp_yakosti_VO_UA_2015.pdf.

11. Розроблення освітніх програм: методичні рекомендації – [Електронний ресурс]. – Режим доступу: http://ihed.org.ua/images/biblioteka/rozroblennya_osv_program_2014_tempusoffice.pdf.

12. Європейська кредитна трансферно-накопичувана система - Довідник користувача – 2015. [Електронний ресурс]. – Режим доступу: http://erasmusplus.org.ua/erasmus/ka3-pidtrymka-reform/natsionalna-komandaekspertiv-here/materiali-here.html

13. Біжан І. В. та ін. Організація навчально-виховного процесу, методичної і наукової роботи у вищій військовій школі. Підручник – Харків: ХВУ, 2001. – 410 с.

Пояснювальна записка

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.		+	+	+
Фахові компетентності				
КФ 1. Здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності.		+		+
КФ 2. Здатність до використання інформаційних і комунікаційних технологій з метою пошуку нової інформації, створення баз даних, аналізу розподілених АС, каналів зв'язку, систем управління процесами, баз даних, оперативного планування роботи систем на основі аналізу інформаційних потоків та їх оптимізації.	+	+		+

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
КФ 3. Здатність здійснювати проектування (розробку) систем, технологій і засобів інформаційної безпеки	+	+		+
КФ 4. Здатність здійснювати протидію несанкціонованому проникненню в ІТ системи і мережі	+	+	+	
КФ 5. Здатність прогнозувати, виявляти та оцінювати стан інформаційної безпеки об’єктів і систем	+	+		+
КФ 6. Здатність відновлювати нормальне функціонування ІТ систем і мереж після здійснення кібернападів, збоїв та відмов	+	+	+	
КФ 7. Здатність виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту обробки інформації в ІТС	+		+	
КФ 8. Здатність проводити техніко-економічного аналіз й обґрунтовувати проектні рішення з забезпечення кібербезпеки	+	+		+
КФ 9. Здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою	+	+	+	
КФ 10. Здатність здійснювати управління інцидентами інформаційної та кібербезпеки	+	+	+	
КФ 11. Здатність здійснювати управління ризиками інформаційної та кібербезпеки	+	+		+
КФ 12. Здатність виконувати моніторинг даних, комп’ютерних зловживань та аномалій	+	+		+

Матриця відповідності визначених результатів навчання та компетентностей

за спеціальністю 125 Кібербезпека

Результати навчання	Компетентності																			
	ІК	Загальні компетентності							Фахові компетентності											
		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	+	+	+	+																
РН-2	+	+	+		+	+														
РН-3	+	+	+		+	+														
РН-4	+	+	+		+	+														
РН-5	+		+		+	+														
РН-6	+		+																	
РН-7	+		+		+				+											
РН-8	+		+		+				+											
РН-9	+					+			+		+	+	+		+	+	+		+	+
РН-10	+	+								+									+	
РН-11	+	+								+									+	
РН-12	+														+					+
РН-13	+					+				+			+			+			+	+
РН-14	+									+	+		+			+		+	+	
РН-15	+									+	+								+	
РН-16	+								+		+				+					+
РН-17	+		+							+	+	+	+	+		+			+	
РН-18	+	+								+	+		+						+	
РН-19	+									+			+			+			+	
РН-20	+									+	+		+	+				+		
РН-21	+	+											+				+		+	
РН-22	+	+											+						+	
РН-23	+												+	+		+			+	
РН-24	+	+										+	+				+		+	
РН-25	+												+			+	+		+	
РН-26	+												+						+	

Результати навчання	Компетентності																				
	ІК	Загальні компетентності							Фахові компетентності												
		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-27	+	+										+	+	+						
РН-28	+					+							+				+			+
РН-29	+					+					+	+	+			+	+			+
РН-30	+																			+
РН-31	+									+				+				+		
РН-32	+	+										+	+			+			+	
РН-33	+								+			+				+	+			+
РН-34	+								+			+	+			+	+			+
РН-35	+	+							+		+	+	+		+	+	+			+
РН-36	+																	+		
РН-37	+													+				+		
РН-38	+													+				+		
РН-39	+																	+		
РН-40	+																	+		
РН-41	+															+			+	
РН-42	+											+	+			+	+		+	+
РН-43	+		+						+			+	+			+	+		+	+
РН-44	+								+			+	+			+	+			+
РН-45	+											+	+			+	+			+
РН-46	+											+	+			+	+			+
РН-47	+									+	+		+					+		
РН-48	+												+	+		+		+	+	
РН-49	+												+	+		+			+	
РН-50	+										+		+			+			+	
РН-51	+												+			+			+	
РН-52	+												+	+		+			+	
РН-53	+																			
РН-54	+	+	+				+	+												

Матриця відповідності освітніх компонентів і компетентностей освітньої програми

Освітні компоненти	Компетентності																			
	ІК	Загальні компетентності							Фахові компетентності											
		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
ПЦ 1	+					+		+			+								+	
ПЦ 2	+		+									+								
ПЦ 3	+							+							+					
ПЦ 4	+	+			+	+				+		+			+					+
ПЦ 5	+	+	+			+			+		+						+		+	
ПЦ 6	+	+				+		+							+					
ПЦ 7	+	+						+												
ПЦ 8	+	+			+			+												
ПЦ 9	+	+								+	+		+							
ПЦ 10	+		+							+	+		+							
ПЦ 11	+									+										
ПЦ 12	+							+						+	+					
ПЦ 13	+									+				+						
ПЦ 14	+							+			+						+			
ПЦ 15	+	+								+										
ПЦ 16	+	+								+	+			+						+
ПЦ 17	+									+	+	+		+			+			+
ПЦ 18	+							+			+									+
ПЦ 19	+				+				+			+					+		+	
ПЦ 20	+	+			+			+												
ПЦ 21	+	+	+							+	+		+							
ПЦ 22	+											+								
ПЦ 23	+	+								+	+	+		+			+			
ПЦ 24	+	+						+	+			+					+			
ПЦ 25	+		+									+								

Освітні компоненти	Компетентності																			
	ІК	Загальні компетентності							Фахові компетентності											
		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
ПЦ 26	+	+			+			+												
ПЦ 27	+			+		+			+											
ПЦ 28	+								+			+								
ПЦ 29		+				+		+												
ПЦ 30	+	+				+														
ПЦ 31	+	+				+	+	+					+	+		+				
МНР 1	+			+			+													
МНР 2	+			+			+													
МНР 3	+			+			+													
МНР 4	+			+			+													
МДР 1.1	+						+			+						+		+		
МДР 1.2	+						+			+						+		+		
МДР 1.3	+						+	+		+								+		+
МДР 1.4	+	+				+				+								+		
МДР 1.5	+	+								+										
МДР 1.6	+	+	+			+								+			+		+	
МДР 1.7	+						+	+					+					+		+
МДР 2.1	+	+	+					+					+			+		+		
МДР 2.2	+		+					+								+		+		
МДР 2.3	+	+						+										+		+
МДР 2.4	+		+			+												+		
МДР 2.5	+	+								+										
МДР 2.6	+	+	+			+								+			+		+	
МДР 2.7	+							+		+										

Матриця відповідності освітніх компонентів і результатів навчання освітньої програми

Освітні компоненти	Результати навчання																																																				
	РН-1	РН-2	РН-3	РН-4	РН-5	РН-6	РН-7	РН-8	РН-9	РН-10	РН-11	РН-12	РН-13	РН-14	РН-15	РН-16	РН-17	РН-18	РН-19	РН-20	РН-21	РН-22	РН-23	РН-24	РН-25	РН-26	РН-27	РН-28	РН-29	РН-30	РН-31	РН-32	РН-33	РН-34	РН-35	РН-36	РН-37	РН-38	РН-39	РН-40	РН-41	РН-42	РН-43	РН-44	РН-45	РН-46	РН-47	РН-48	РН-49	РН-50	РН-51	РН-52	РН-53	РН-54
ПЦ 1		+	+	+	+				+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+			+			+						+	+	+	+			+		+	+	+	+		
ПЦ 2	+	+	+	+	+	+	+	+	+								+							+			+		+			+	+	+	+							+	+	+	+	+								+
ПЦ 3									+			+				+																			+																			+
ПЦ 4	+	+	+	+			+	+	+	+	+	+	+	+	+	+	+	+		+	+	+		+			+	+	+	+	+	+	+	+	+							+	+	+	+	+	+							+
ПЦ 5	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+		+	+	+	+								+	+			+	+	+	+	+	+		+
ПЦ 6	+	+	+	+	+				+	+	+	+	+			+		+			+	+		+			+	+	+			+			+																			+
ПЦ 7	+	+	+	+						+	+							+			+	+		+			+					+			+																			+
ПЦ 8	+	+	+	+	+		+	+		+	+							+			+	+		+			+					+			+																			+
ПЦ 9	+	+	+	+					+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+		+	+							+	+	+	+	+	+	+	+	+	+	+		+
ПЦ 10	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+		+	+							+	+	+	+	+	+	+	+	+	+	+		+
ПЦ 11										+	+		+	+	+		+	+	+	+											+																+							
ПЦ 12									+			+				+	+			+			+				+				+				+		+	+										+	+			+		+
ПЦ 13										+	+		+	+	+		+	+	+	+			+				+				+						+	+									+	+	+			+		
ПЦ 14									+					+	+	+	+	+		+								+	+				+	+	+							+	+	+	+	+	+			+				+
ПЦ 15	+	+	+	+						+	+		+	+	+		+	+	+	+	+	+		+			+				+	+			+												+							+
ПЦ 16	+	+	+	+					+	+	+		+	+	+	+	+	+	+	+	+	+	+	+			+	+	+	+	+	+	+	+	+							+	+	+	+	+	+	+	+	+		+		+
ПЦ 17									+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+		+	+	+	+	+	+	+	+	+		+	+				+	+	+	+	+	+	+	+	+		+		
ПЦ 18									+			+	+	+	+	+	+	+		+								+	+	+			+	+	+							+	+	+	+	+	+			+				+
ПЦ 19		+	+	+	+		+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			+	+	+	+						+	+	+	+	+	+		+	+	+	+	+		
ПЦ 20	+	+	+	+	+		+	+		+	+							+			+	+		+			+					+			+																			+
ПЦ 21	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+		+	+							+	+	+	+	+	+	+	+	+	+	+		+
ПЦ 22									+								+							+			+		+			+	+	+	+							+	+	+	+	+								
ПЦ 23	+	+	+	+					+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+		+	+	+	+	+		+	+				+	+	+	+	+	+	+	+	+		+		+
ПЦ 24	+	+	+	+			+	+	+	+	+					+	+	+			+	+		+	+		+	+	+			+	+	+	+							+	+	+	+	+								+
ПЦ 25	+	+	+	+	+	+	+	+	+								+							+			+		+			+	+	+	+							+	+	+	+	+								+

Освітні компоненти	Результати навчання																																																				
	РН-1	РН-2	РН-3	РН-4	РН-5	РН-6	РН-7	РН-8	РН-9	РН-10	РН-11	РН-12	РН-13	РН-14	РН-15	РН-16	РН-17	РН-18	РН-19	РН-20	РН-21	РН-22	РН-23	РН-24	РН-25	РН-26	РН-27	РН-28	РН-29	РН-30	РН-31	РН-32	РН-33	РН-34	РН-35	РН-36	РН-37	РН-38	РН-39	РН-40	РН-41	РН-42	РН-43	РН-44	РН-45	РН-46	РН-47	РН-48	РН-49	РН-50	РН-51	РН-52	РН-53	РН-54
ПЦ 26	+	+	+	+	+		+	+		+	+							+			+	+		+			+					+			+																			+
ПЦ 27	+	+	+	+	+		+	+	+				+			+												+					+	+	+								+	+										
ПЦ 28							+	+	+							+	+							+			+		+			+	+	+								+	+	+	+	+								
ПЦ 29	+	+	+	+	+				+	+	+		+					+			+	+		+			+	+	+			+			+																			+
ПЦ 30	+	+	+	+	+				+	+	+		+					+			+	+		+			+	+				+			+																			+
ПЦ 31	+	+	+	+	+				+	+	+		+	+			+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+		+	+			+	+	+	+	+	+	+	+	+	+	+	+		+
МНР 1	+																																																					+
МНР 2	+																																																					+
МНР 3	+																																																					+
МНР 4	+																																																					+
МДР 1.1									+	+	+		+	+	+		+	+	+	+			+		+				+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+
МДР 1.2									+	+	+		+	+	+		+	+	+	+			+		+				+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+
МДР 1.3									+	+	+	+	+	+	+	+	+	+	+	+			+		+			+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+
МДР 1.4	+	+	+	+	+				+	+	+		+	+	+		+	+	+	+	+	+		+			+	+	+		+	+			+												+							+
МДР 1.5	+	+	+	+						+	+		+	+	+		+	+	+	+	+	+		+			+				+	+			+												+							+
МДР 1.6	+	+	+	+	+	+	+	+	+	+	+		+				+	+		+	+	+	+	+			+	+	+		+	+	+	+	+		+	+			+	+	+	+	+	+		+	+	+	+	+		+
МДР 1.7									+			+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+
МДР 2.1	+	+	+	+	+	+	+	+	+	+	+		+	+			+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+		+
МДР 2.2	+	+	+	+	+	+	+	+	+				+	+			+		+	+			+		+				+		+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+		+	+	+		+
МДР 2.3	+	+	+	+					+	+	+	+	+	+		+		+		+	+	+		+			+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+						+
МДР 2.4	+	+	+	+	+	+	+						+	+			+			+								+	+		+					+	+	+	+	+			+				+	+						
МДР 2.5	+	+	+	+						+	+		+	+	+		+	+	+	+	+	+		+			+				+	+			+												+							+
МДР 2.6	+	+	+	+	+	+	+	+	+	+	+		+				+	+		+	+	+	+	+			+	+	+		+	+	+	+	+		+	+			+	+	+	+	+	+		+	+	+	+	+		+
МДР 2.7										+	+		+	+	+		+	+	+	+											+																+							+