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

УХВАЛЕНО
Рішенням вченої ради
Харківського національного
економічного університету
імені Семена Кузнеця
від 23.09.2020 року протокол № 2

ВВЕДЕНО В ДІЮ
Наказом в. о. ректора Харківського
національного економічного університету
імені Семена Кузнеця
від 24.09.2020 року № 172

Володимир ПОНОМАРЕНКО

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
"КІБЕРБЕЗПЕКА"

(назва ОПП)

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

ХАРКІВ, 2020

ПРЕАМБУЛА

Склад робочої групи освітньо-професійної програми “Кібербезпека”:

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, кандидат 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.

Освітньо-професійну програму “Кібербезпека” оновлено на підставі:

1. Законодавчих та нормативних актів: Законів України “Про освіту”, Національної рамки кваліфікації, Національного класифікатору України: Класифікатор професій (ДК 003:2010).
2. Аналізу ринку праці, з урахуванням регіонального контексту.
3. Вивчення вітчизняного та зарубіжного досвіду.
4. Пропозицій роботодавців.
5. Стандарту вищої освіти України: перший (бакалаврський) рівень, галузь знань 12 – Інформаційні технології, спеціальність 125 – Кібербезпека.

Рецензії-відгуки зовнішніх стейкхолдерів (додаються).

І. Загальна характеристика

Рівень вищої освіти	Перший (бакалаврський) рівень
Ступінь, що присвоюється	Бакалавр
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня програма	Кібербезпека / Cyber Security
Обмеження щодо форм навчання	немає
Освітня кваліфікація	Бакалавр з кібербезпеки
Кваліфікація(-ї) професійна(-і)	Відсутня
Кваліфікація в дипломі	Ступінь вищої освіти − Бакалавр Спеціальність – 125 Кібербезпека Освітня програма – Кібербезпека
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).
Академічні права випускників	Можливість продовжити навчання за освітньою програмою ступеня магістра.
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.

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).

ІІІ – Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання за спеціальністю 125 "Кібербезпека" освітньо-професійної програми "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.

IV. Структура освітньо-професійної програми підготовки бакалаврів

4.1 Обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти

Обсяг освітньо-професійної програми підготовки бакалавра галузі знань 12 "Інформаційні технології" спеціальності 125 "Кібербезпека" освітньо-професійної програми "Кібербезпека":

- на базі повної загальної середньої освіти – 240 кредитів ЄКТС. Термін навчання: денна форма – 3 роки 10 місяців; заочна форма – 4 роки 10 місяців.

- на базі ступеня "молодший бакалавр" (освітньо-кваліфікаційного рівня "молодший спеціаліст") – 240 кредитів ЄКТС, заклад вищої освіти має право визнати та перезарахувати не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста). Термін навчання: денна форма – 2 роки 10 місяців; заочна форма – 2 роки 10 місяців.

4.2 Структура освітньо-професійної програми підготовки бакалаврів

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ПІДГОТОВКИ БАКАЛАВРІВ

Галузь знань 12 "Інформаційні технології", спеціальність: 125 "Кібербезпека", освітньо-професійна програма "Кібербезпека"

Складові освітньо-професійної програми	Загальна кількість		Структура, %
	кредитів ЄКТС	годин	
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ	**29**	**870**	**12%**
ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ	*24*	*720*	*10%*
ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ	*5*	*150*	*2%*
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ	**211**	**6330**	**88%**
ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ	*155*	*4650*	*65%*
ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ	*56*	*1680*	*23%*
ЗАГАЛЬНА КІЛЬКІСТЬ :	**240**	**7200**	**100%**
в тому числі: вибіркові освітні компоненти	*61*	*1830*	*25%*

Код ОК	Освітні компоненти
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ	
ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ	
ОК1	Українська мова (за професійним спрямуванням)
ОК2	Іноземна мова (за професійним спрямуванням)
ОК3	Соціальна та економічна історія України
ОК4	Філософія

ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ	
ВК 1	Дисципліна правового спрямування
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ	
ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ	
ОК5	Вища математика
ОК6	Вступ до фаху
ОК7	Розробка та аналіз алгоритмів
ОК8	Фізичні основи технічних засобів розвідки
ОК9	Інформаційна безпека держави
ОК10	Основи програмування
ОК11	Навчальна практика “університетська освіта”
ОК12	Тренінг-курс “Безпека життєдіяльності”
ОК13	Математичні основи криптології
ОК14	Теоретичні основи криптографії
ОК15	Основи побудови та захисту сучасних операційних систем
ОК16	Технології програмування
ОК17	Основи побудови та захисту мікропроцесорних систем
ОК18	Менеджмент інформаційної безпеки
ОК19	Курсовий проект: введення в мережі
ОК20	Введення в мережі
ОК21	Інформаційні системи та інтернет технології
ОК22	Основи математичного моделювання
ОК23	Організація та інформаційне забезпечення управлінської діяльності
ОК24	Виробнича практика
ОК25	Основи криптографічного захисту
ОК26	Комплексні системи захисту інформації
ОК27	Безпека в інформаційно-комунікаційних системах
ОК28	Комплексний курсовий проект
ОК29	Основи стеганографічного захисту інформації
ОК30	Тренінг-курс “Основи охорони праці”

ОК31	Іноземна мова академічної та професійної комунікації
ОК32	Організаційне забезпечення захисту інформації
ОК33	Комплексний тренінг
ОК34	Переддипломна практика
ОК35	Дипломний проект
ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ	
ВК2	Майнор або вільний майнор
ВК3	Майнор або вільний майнор
ВК4	Майнор або вільний майнор
ВК5	Майнор або вільний майнор
Студенти обирають один із запропонованих мейджорів **МЕЙДЖОР 1**	
ВК6	Корпоративні мережі та системи доступу
ВК7	Безпека та аудит бездротових та рухомих мереж
ВК8	Основи планування та адміністрування служб доступу до інформаційних ресурсів
ВК9	Адміністрування Unix-подібних систем
ВК10	Мережне програмування
ВК11	Основи технічного захисту інформації
ВК12	Експертні системи
МЕЙДЖОР 2	
ВК6	Blockchain: основи та приклади застосування
ВК7	Основи смарт-контрактів
ВК8	Основи розробки децентралізованих застосувань (decentralized applications (dapps))
ВК9	Безпека банківських систем
ВК10	Безпека в Devops
ВК11	Основи технічного захисту інформації
ВК12	Організація і збереження баз даних

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.

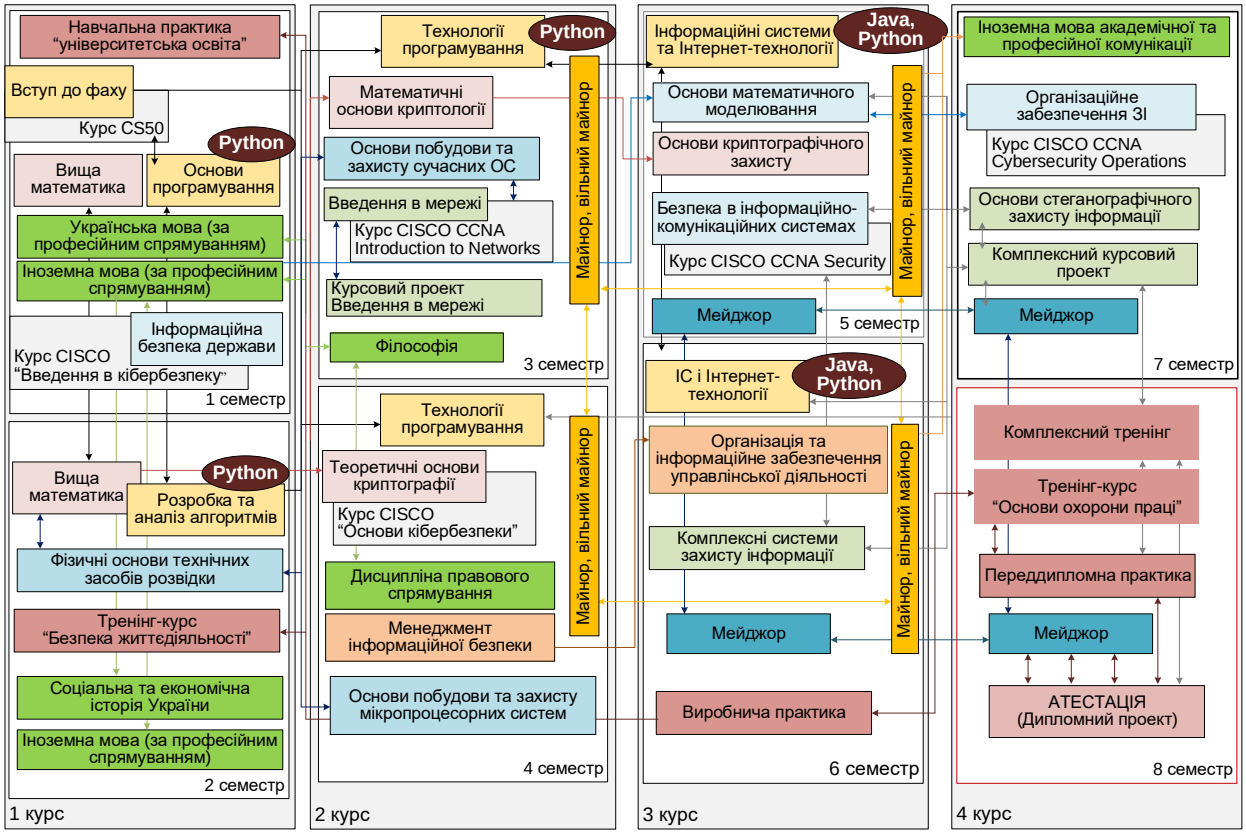
– МЕЙДЖОР – профільні навчальні дисципліни освітньо-професійної програми, які поглиблюють професійну підготовку за певною спеціалізацією.

– Дисципліна правового спрямування – окрема дисципліна з обсягом 5 кредитів ЄКТС.

Загальний обсяг МАЙНОРІВ складає 20 кредитів ЄКТС (по 5 кредитів на дисципліну). Загальний обсяг МЕЙДЖЕРУ складає 36 кредитів ЄКТС.

4.3 Структурно-логічна схема освітньо-професійної програми

Структурно-логічна схема освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти



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 проєкту) 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 вищих навчальних закладів, 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 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: 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 педагогічних, наукових і науково-педагогічних працівників	Педагогічні і науково-педагогічні працівники Університету можуть підвищувати кваліфікацію за різними формами, видами 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 навчальних 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. Внутрішнє 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 навчальних 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	Достовірна, об'єктивна, актуальна, своєчасна та легкодоступна інформація за освітньо-професійною програмою "Кібербезпека" публікується на сайті ХНЕУ

кваліфікації	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.
Дотримання академічної доброчесності працівниками закладу вищої освіти та здобувачами 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 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:

2) на основі повної загальної середньої освіти – у формі зовнішнього незалежного оцінювання. У 2020 році приймаються сертифікати зовнішнього незалежного оцінювання 2017, 2018, 2019 та 2020 років, крім оцінок з англійської, французької, німецької та іспанської мов. Якщо конкурсний предмет обрано іноземну мову, вступник має право подавати оцінку із сертифікатів 2018 – 2020 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 (К1 = 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, фахового вступного випробування в усній формі. У 2020 році приймаються сертифікати зовнішнього незалежного оцінювання 2017–2020 років.

Конкурсний бал обчислюється за формулою:

Конкурсний бал (КБ) = П1 + П2,

де П1 – оцінки зовнішнього незалежного оцінювання з української мови і літератури або вступного іспиту з української мови і літератури. Мінімальна кількість балів, з якими вступник допускається до участі у конкурсі – 100 балів. П2 – 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.

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

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.	+	+		+

Таблиця 2

Матриця відповідності визначених результатів навчання, компетентностей та освітніх компонентів

Результати навчання	Компетентності																				
	ІК	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	ОК8 ОК9 ОК13 ОК14 ОК20 ОК25 ОК27 ОК28 ОК29 ОК33 ОК35	ОК1 ОК4 ОК11 ОК12 ОК24 ОК30 ОК34 ОК35 ВК2 ВК3 ВК4 ВК5	ОК6 ОК9 ОК13 ОК14 ОК18 ОК21 ОК26 ОК27 ОК28 ОК32 ОК33 ОК34 ОК35 ВК2 ВК3 ВК4 ВК5	ОК1 ОК2 ОК31 ВК2 ВК3 ВК4 ВК5																
РН-2	ОК8 ОК9 ОК13 ОК14 ОК20 ОК23 ОК25 ОК27 ОК28 ОК29 ОК33 ОК35	ОК1 ОК4 ОК11 ОК12 ОК24 ОК30 ОК34 ОК35 ВК2 ВК3 ВК4 ВК5	ОК6 ОК9 ОК13 ОК14 ОК18 ОК21 ОК26 ОК27 ОК28 ОК32 ОК33 ОК34 ОК35 ВК2 ВК3 ВК4 ВК5		ОК12 ОК24 ОК30	ОК4 ОК33 ОК34 ОК35														
РН-3	ОК8 ОК9	ОК1 ОК4	ОК6 ОК9		ОК12 ОК24	ОК4 ОК33															

	ОК13 ОК14 ОК20 ОК23 ОК25 ОК27 ОК28 ОК29 ОК33 ОК35	ОК11 ОК12 ОК24 ОК30 ОК34 ОК35 ВК2 ВК3 ВК4 ВК5	ОК13 ОК14 ОК18 ОК21 ОК26 ОК27 ОК28 ОК32 ОК33 ОК34 ОК35 ВК2 ВК3 ВК4 ВК5		ОК30	ОК34 ОК35														
РН-4	ОК8 ОК9 ОК13 ОК14 ОК20 ОК23 ОК25 ОК27 ОК28 ОК29 ОК33 ОК35	ОК1 ОК4 ОК11 ОК12 ОК24 ОК30 ОК34 ОК35 ВК2 ВК3 ВК4 ВК5	ОК6 ОК9 ОК13 ОК14 ОК18 ОК21 ОК26 ОК27 ОК28 ОК32 ОК33 ОК34 ОК35 ВК2 ВК3 ВК4 ВК5		ОК12 ОК24 ОК30	ОК4 ОК33 ОК34 ОК35														
РН-5	ОК9 ОК14 ОК23 ОК25 ОК29 ОК33 ОК35		ОК6 ОК9 ОК13 ОК14 ОК18 ОК21 ОК26 ОК27 ОК28 ОК32 ОК33		ОК12 ОК24 ОК30	ОК4 ОК33 ОК34 ОК35														

			ОК34 ОК35 ВК2 ВК3 ВК4 ВК5																	
РН-6	ОК9 ОК14 ОК25 ОК29		ОК6 ОК9 ОК13 ОК14 ОК18 ОК21 ОК26 ОК27 ОК28 ОК32 ОК33 ОК34 ОК35 ВК2 ВК3 ВК4 ВК5																	
РН-7	ОК8 ОК9 ОК14 ОК23 ОК25 ОК28 ОК29 ОК32		ОК6 ОК9 ОК13 ОК14 ОК18 ОК21 ОК26 ОК27 ОК28 ОК32 ОК33 ОК34 ОК35 ВК2 ВК3 ВК4 ВК5		ОК12 ОК24 ОК30				ОК9 ОК23 ОК28 ОК32 ВК1											
РН-8	ОК8 ОК9 ОК14		ОК6 ОК9 ОК13		ОК12 ОК24 ОК30				ОК9 ОК23 ОК28											

	ОК23 ОК25 ОК28 ОК29 ОК32		ОК14 ОК18 ОК21 ОК26 ОК27 ОК28 ОК32 ОК33 ОК34 ОК35 БК2 БК3 БК4 БК5						ОК32 БК1										
РН-9	ОК7 ОК8 ОК9 ОК13 ОК14 ОК16 ОК18 ОК20 ОК21 ОК22 ОК23 ОК25 ОК26 ОК27 ОК28 ОК29 ОК32 ОК33 ОК35					ОК4 ОК33 ОК34 ОК35			ОК9 ОК23 ОК28 ОК32 БК1		ОК5 ОК9 ОК13 ОК14 ОК18 ОК20 ОК21 ОК22 ОК25	ОК6 ОК7 ОК8 ОК21 ОК23 ОК26 ОК27 ОК28 ОК32	ОК13 ОК14 ОК15 ОК25 ОК35 БК6 БК7 БК8 БК9 БК10 БК11 БК12		ОК7 ОК8 ОК10 ОК16	ОК35 БК6 БК7 БК8 БК9 БК10 БК11 БК12	ОК9 ОК18 ОК21 ОК23 ОК27 ОК28 ОК29		ОК5 ОК9 ОК23	ОК8 ОК20 ОК21 ОК22
РН-10	ОК8 ОК9 ОК13 ОК14 ОК15 ОК17 ОК20 ОК21 ОК23 ОК25	ОК1 ОК4 ОК11 ОК12 ОК24 ОК30 ОК34 ОК35 БК2 БК3								ОК8 ОК13 ОК14 ОК17 ОК19 ОК20 ОК21 ОК25 ОК27									ОК5 ОК9 ОК23	

	ОК27 ОК28 ОК33 ОК35	ВК4 ВК5																	
РН-11	ОК8 ОК9 ОК13 ОК14 ОК15 ОК17 ОК20 ОК21 ОК23 ОК25 ОК27 ОК28 ОК33 ОК35	ОК1 ОК4 ОК11 ОК12 ОК24 ОК30 ОК34 ОК35 ВК2 ВК3 ВК4 ВК5								ОК8 ОК13 ОК14 ОК17 ОК19 ОК20 ОК21 ОК25 ОК27									ОК5 ОК9 ОК23	
РН-12	ОК7 ОК8 ОК16 ОК17 ОК21 ОК22 ОК23														ОК7 ОК8 ОК10 ОК16					ОК8 ОК20 ОК21 ОК22
РН-13	ОК8 ОК9 ОК13 ОК14 ОК15 ОК17 ОК20 ОК21 ОК22 ОК23 ОК25 ОК27 ОК33 ОК35					ОК4 ОК33 ОК34 ОК35				ОК8 ОК13 ОК14 ОК17 ОК19 ОК20 ОК21 ОК25 ОК27			ОК13 ОК14 ОК15 ОК25 ОК35 ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12			ОК35 ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12			ОК5 ОК9 ОК23	ОК8 ОК20 ОК21 ОК22
РН-14	ОК8 ОК9 ОК13 ОК14									ОК8 ОК13 ОК14 ОК17	ОК5 ОК9 ОК13 ОК14		ОК13 ОК14 ОК15 ОК25			ОК35 ВК6 ВК7 ВК8		ОК33 ОК34 ВК6 ВК7	ОК5 ОК9 ОК23	

	ОК15 ОК17 ОК18 ОК20 ОК21 ОК22 ОК23 ОК25 ОК27 ОК35									ОК19 ОК20 ОК21 ОК25 ОК27	ОК18 ОК20 ОК21 ОК22 ОК25		ОК35 БК6 БК7 БК8 БК9 БК10 БК11 БК12			БК9 БК10 БК11 БК12		БК8 БК9 БК10 БК11 БК12		
РН-15	ОК8 ОК9 ОК13 ОК14 ОК15 ОК17 ОК18 ОК20 ОК21 ОК22 ОК23 ОК25 ОК27									ОК8 ОК13 ОК14 ОК17 ОК19 ОК20 ОК21 ОК25 ОК27	ОК5 ОК9 ОК13 ОК14 ОК18 ОК20 ОК21 ОК22 ОК25								ОК5 ОК9 ОК23	
РН-16	ОК7 ОК8 ОК9 ОК13 ОК14 ОК16 ОК18 ОК20 ОК21 ОК22 ОК23 ОК25 ОК27 ОК28 ОК32								ОК9 ОК23 ОК28 ОК32 БК1		ОК5 ОК9 ОК13 ОК14 ОК18 ОК20 ОК21 ОК22 ОК25				ОК7 ОК8 ОК10 ОК16				ОК8 ОК20 ОК21 ОК22
РН-17	ОК8 ОК9 ОК13 ОК14 ОК15		ОК6 ОК9 ОК13 ОК14 ОК18							ОК8 ОК13 ОК14 ОК17 ОК19	ОК5 ОК9 ОК13 ОК14 ОК18	ОК6 ОК7 ОК8 ОК21 ОК23	ОК13 ОК14 ОК15 ОК25 ОК35	ОК16 ОК17 ОК20 ОК21 ОК27		ОК35 БК6 БК7 БК8 БК9			ОК5 ОК9 ОК23	

	ОК16 ОК17 ОК18 ОК20 ОК21 ОК22 ОК23 ОК25 ОК26 ОК27 ОК28 ОК29 ОК32 ОК35		ОК21 ОК26 ОК27 ОК28 ОК32 ОК33 ОК34 ОК35 БК2 БК3 БК4 БК5							ОК20 ОК21 ОК25 ОК27	ОК20 ОК21 ОК22 ОК25	ОК26 ОК27 ОК28 ОК32	БК6 БК7 БК8 БК9 БК10 БК11 БК12	ОК35		БК10 БК11 БК12				
РН-18	ОК8 ОК9 ОК13 ОК14 ОК15 ОК17 ОК18 ОК20 ОК21 ОК22 ОК23 ОК25 ОК27 ОК28 ОК33 ОК35	ОК1 ОК4 ОК11 ОК12 ОК24 ОК30 ОК34 ОК35 БК2 БК3 БК4 БК5								ОК8 ОК13 ОК14 ОК17 ОК19 ОК20 ОК21 ОК25 ОК27	ОК5 ОК9 ОК13 ОК14 ОК18 ОК20 ОК21 ОК22 ОК25		ОК13 ОК14 ОК15 ОК25 ОК35 БК6 БК7 БК8 БК9 БК10 БК11 БК12						ОК5 ОК9 ОК23	
РН-19	ОК13 ОК14 ОК15 ОК17 ОК20 ОК21 ОК23 ОК25 ОК27 ОК35	ОК1 ОК4 ОК11 ОК12 ОК24 ОК30 ОК34 ОК35 БК2 БК3 БК4 БК5								ОК8 ОК13 ОК14 ОК17 ОК19 ОК20 ОК21 ОК25 ОК27			ОК13 ОК14 ОК15 ОК25 ОК35 БК6 БК7 БК8 БК9 БК10 БК11 БК12			ОК35 БК6 БК7 БК8 БК9 БК10 БК11 БК12			ОК5 ОК9 ОК23	
РН-20	ОК8	ОК1								ОК8	ОК5		ОК13	ОК16				ОК33		

	ОК9 ОК13 ОК14 ОК15 ОК16 ОК17 ОК18 ОК20 ОК21 ОК22 ОК23 ОК25 ОК27 ОК35	ОК4 ОК11 ОК12 ОК24 ОК30 ОК34 ОК35 ВК2 ВК3 ВК4 ВК5								ОК13 ОК14 ОК17 ОК19 ОК20 ОК21 ОК25 ОК27	ОК9 ОК13 ОК14 ОК18 ОК20 ОК21 ОК22 ОК25		ОК14 ОК15 ОК25 ОК35 ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12	ОК17 ОК20 ОК21 ОК27 ОК35				ОК34 ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12		
РН-21	ОК8 ОК9 ОК13 ОК14 ОК20 ОК21 ОК23 ОК25 ОК27 ОК28 ОК33 ОК35	ОК1 ОК4 ОК11 ОК12 ОК24 ОК30 ОК34 ОК35 ВК2 ВК3 ВК4 ВК5											ОК13 ОК14 ОК15 ОК25 ОК35 ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12				ОК9 ОК18 ОК21 ОК23 ОК27 ОК28 ОК29		ОК5 ОК9 ОК23	
РН-22	ОК8 ОК9 ОК13 ОК14 ОК20 ОК23 ОК25 ОК27 ОК28 ОК33 ОК35	ОК1 ОК4 ОК11 ОК12 ОК24 ОК30 ОК34 ОК35											ОК13 ОК14 ОК15 ОК25 ОК35 ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12						ОК5 ОК9 ОК23	
РН-23	ОК9 ОК13 ОК14 ОК16 ОК17												ОК13 ОК14 ОК15 ОК25 ОК35	ОК16 ОК17 ОК20 ОК21 ОК27		ОК35 ВК6 ВК7 ВК8 ВК9			ОК5 ОК9 ОК23	

	ОК20 ОК21 ОК23 ОК25 ОК27 ОК35												ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12	ОК35		ВК10 ВК11 ВК12				
РН-24	ОК8 ОК9 ОК13 ОК14 ОК20 ОК21 ОК23 ОК25 ОК26 ОК27 ОК28 ОК29 ОК32 ОК33 ОК35	ОК1 ОК4 ОК11 ОК12 ОК24 ОК30 ОК34 ОК35 ВК2 ВК3 ВК4 ВК5										ОК6 ОК7 ОК8 ОК21 ОК23 ОК26 ОК27 ОК28 ОК32	ОК13 ОК14 ОК15 ОК25 ОК35 ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12				ОК9 ОК18 ОК21 ОК23 ОК27 ОК28 ОК29		ОК5 ОК9 ОК23	
РН-25	ОК9 ОК13 ОК14 ОК20 ОК21 ОК23 ОК25 ОК28 ОК35												ОК13 ОК14 ОК15 ОК25 ОК35 ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12			ОК35 ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12	ОК9 ОК18 ОК21 ОК23 ОК27 ОК28 ОК29		ОК5 ОК9 ОК23	
РН-26	ОК9 ОК13 ОК14 ОК23 ОК25 ОК35												ОК13 ОК14 ОК15 ОК25 ОК35 ВК6 ВК7 ВК8 ВК9						ОК5 ОК9 ОК23	

													BK10 BK11 BK12						
РН-27	ОК8 ОК9 ОК13 ОК14 ОК16 ОК17 ОК21 ОК23 ОК25 ОК26 ОК27 ОК28 ОК29 ОК32 ОК33 ОК35	ОК1 ОК4 ОК11 ОК12 ОК24 ОК30 ОК34 ОК35 БК2 БК3 БК4 БК5										ОК6 ОК7 ОК8 ОК21 ОК23 ОК26 ОК27 ОК28 ОК32	ОК13 ОК14 ОК15 ОК25 ОК35 БК6 БК7 БК8 БК9 БК10 БК11 БК12	ОК16 ОК17 ОК20 ОК21 ОК27 ОК35						
РН-28	ОК8 ОК9 ОК13 ОК14 ОК18 ОК20 ОК21 ОК22 ОК23 ОК25 ОК27 ОК28 ОК33 ОК35					ОК4 ОК33 ОК34 ОК35							ОК13 ОК14 ОК15 ОК25 ОК35 БК6 БК7 БК8 БК9 БК10 БК11 БК12				ОК9 ОК18 ОК21 ОК23 ОК27 ОК28 ОК29			ОК8 ОК20 ОК21 ОК22
РН-29	ОК8 ОК9 ОК13 ОК14 ОК18 ОК20 ОК21 ОК22 ОК23 ОК25										ОК5 ОК9 ОК13 ОК14 ОК18 ОК20 ОК21 ОК22 ОК25 ОК27	ОК6 ОК7 ОК8 ОК21 ОК23 ОК26 ОК27 ОК28 ОК32	ОК13 ОК14 ОК15 ОК25 ОК35 БК6 БК7 БК8 БК9 БК10			ОК35 БК6 БК7 БК8 БК9 БК10 БК11 БК12	ОК9 ОК18 ОК21 ОК23 ОК27 ОК28 ОК29			ОК8 ОК20 ОК21 ОК22

	ОК26 ОК27 ОК28 ОК29 ОК32 ОК33 ОК35												ВК11 ВК12							
РН-30	ОК8 ОК9 ОК20 ОК21 ОК22																			ОК8 ОК20 ОК21 ОК22
РН-31	ОК8 ОК13 ОК14 ОК15 ОК16 ОК17 ОК20 ОК21 ОК25 ОК27 ОК35									ОК8 ОК13 ОК14 ОК17 ОК19 ОК20 ОК21 ОК25 ОК27				ОК16 ОК17 ОК20 ОК21 ОК27 ОК35				ОК33 ОК34 ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12		
РН-32	ОК8 ОК9 ОК13 ОК14 ОК20 ОК21 ОК23 ОК25 ОК26 ОК27 ОК28 ОК29 ОК32 ОК33 ОК35	ОК1 ОК4 ОК11 ОК12 ОК24 ОК30 ОК34 ОК35 ВК2 ВК3 ВК4 ВК5										ОК6 ОК7 ОК8 ОК21 ОК23 ОК26 ОК27 ОК28 ОК32	ОК13 ОК14 ОК15 ОК25 ОК35 ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12			ОК35 ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12			ОК5 ОК9 ОК23	
РН-33	ОК8								ОК9			ОК6				ОК35	ОК9			ОК8

	ОК9 ОК18 ОК20 ОК21 ОК22 ОК23 ОК26 ОК27 ОК28 ОК29 ОК32 ОК35								ОК23 ОК28 ОК32 ВК1			ОК7 ОК8 ОК21 ОК23 ОК26 ОК27 ОК28 ОК32				ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12	ОК18 ОК21 ОК23 ОК27 ОК28 ОК29			ОК20 ОК21 ОК22
РН-34	ОК8 ОК9 ОК13 ОК14 ОК18 ОК20 ОК21 ОК22 ОК23 ОК25 ОК26 ОК27 ОК28 ОК29 ОК32 ОК35								ОК9 ОК23 ОК28 ОК32 ВК1			ОК6 ОК7 ОК8 ОК21 ОК23 ОК26 ОК27 ОК28 ОК32	ОК13 ОК14 ОК15 ОК25 ОК35 ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12			ОК35 ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12	ОК9 ОК18 ОК21 ОК23 ОК27 ОК28 ОК29			ОК8 ОК20 ОК21 ОК22
РН-35	ОК7 ОК8 ОК9 ОК13 ОК14 ОК16 ОК18 ОК20 ОК21 ОК22 ОК23 ОК25 ОК26 ОК27 ОК28	ОК1 ОК4 ОК11 ОК12 ОК24 ОК30 ОК34 ОК35 ВК2 ВК3 ВК4 ВК5							ОК9 ОК23 ОК28 ОК32 ВК1		ОК5 ОК9 ОК13 ОК14 ОК18 ОК20 ОК21 ОК22 ОК25	ОК6 ОК7 ОК8 ОК21 ОК23 ОК26 ОК27 ОК28 ОК32	ОК13 ОК14 ОК15 ОК25 ОК35 ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12		ОК7 ОК8 ОК10 ОК16	ОК35 ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12	ОК9 ОК18 ОК21 ОК23 ОК27 ОК28 ОК29			ОК8 ОК20 ОК21 ОК22

	ОК29 ОК33 ОК35																		
РН-36																	ОК33 ОК34 ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12		
РН-37	ОК16 ОК17 ОК21 ОК27 ОК35													ОК16 ОК17 ОК20 ОК21 ОК27 ОК35				ОК33 ОК34 ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12		
РН-38	ОК16 ОК17 ОК21 ОК27 ОК35													ОК16 ОК17 ОК20 ОК21 ОК27 ОК35				ОК33 ОК34 ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12		
РН-39																	ОК33 ОК34 ВК6 ВК7 ВК8 ВК9 ВК10 ВК11 ВК12		
РН-40																	ОК33 ОК34 ВК6 ВК7		

																		BK8 BK9 BK10 BK11 BK12		
PH-41	OK23 OK35															OK35 BK6 BK7 BK8 BK9 BK10 BK11 BK12			OK5 OK9 OK23	
PH-42	OK8 OK13 OK14 OK18 OK20 OK21 OK22 OK23 OK25 OK26 OK27 OK28 OK29 OK32 OK35											OK6 OK7 OK8 OK21 OK23 OK26 OK27 OK28 OK32	OK13 OK14 OK15 OK25 OK35 BK6 BK7 BK8 BK9 BK10 BK11 BK12			OK35 BK6 BK7 BK8 BK9 BK10 BK11 BK12	OK9 OK18 OK21 OK23 OK27 OK28 OK29		OK5 OK9 OK23	OK8 OK20 OK21 OK22
PH-43	OK8 OK9 OK13 OK14 OK18 OK20 OK21 OK22 OK23 OK25 OK26 OK27 OK28 OK29 OK32		OK6 OK9 OK13 OK14 OK18 OK21 OK26 OK27 OK28 OK32 OK33 OK34 OK35 BK2 BK3						OK9 OK23 OK28 OK32 BK1			OK6 OK7 OK8 OK21 OK23 OK26 OK27 OK28 OK32	OK13 OK14 OK15 OK25 OK35 BK6 BK7 BK8 BK9 BK10 BK11 BK12			OK35 BK6 BK7 BK8 BK9 BK10 BK11 BK12	OK9 OK18 OK21 OK23 OK27 OK28 OK29		OK5 OK9 OK23	OK8 OK20 OK21 OK22

	OK35		BK4 BK5																
PH-44	OK8 OK9 OK13 OK14 OK18 OK20 OK21 OK22 OK23 OK25 OK26 OK27 OK28 OK29 OK32 OK35								OK9 OK23 OK28 OK32 BK1			OK6 OK7 OK8 OK21 OK23 OK26 OK27 OK28 OK32	OK13 OK14 OK15 OK25 OK35 BK6 BK7 BK8 BK9 BK10 BK11 BK12			OK35 BK6 BK7 BK8 BK9 BK10 BK11 BK12	OK9 OK18 OK21 OK23 OK27 OK28 OK29			OK8 OK20 OK21 OK22
PH-45	OK8 OK13 OK14 OK18 OK20 OK21 OK22 OK23 OK25 OK26 OK27 OK28 OK29 OK32 OK35											OK6 OK7 OK8 OK21 OK23 OK26 OK27 OK28 OK32	OK13 OK14 OK15 OK25 OK35 BK6 BK7 BK8 BK9 BK10 BK11 BK12			OK35 BK6 BK7 BK8 BK9 BK10 BK11 BK12	OK9 OK18 OK21 OK23 OK27 OK28 OK29			OK8 OK20 OK21 OK22
PH-46	OK8 OK13 OK14 OK18 OK20 OK21 OK22 OK23 OK25 OK26											OK6 OK7 OK8 OK21 OK23 OK26 OK27 OK28 OK32	OK13 OK14 OK15 OK25 OK35 BK6 BK7 BK8 BK9 BK10			OK35 BK6 BK7 BK8 BK9 BK10 BK11 BK12	OK9 OK18 OK21 OK23 OK27 OK28 OK29			OK8 OK20 OK21 OK22

	OK27 OK28 OK29 OK32 OK35												BK11 BK12						
PH-47	OK8 OK9 OK13 OK14 OK15 OK17 OK18 OK20 OK21 OK22 OK25 OK27 OK35									OK8 OK13 OK14 OK17 OK19 OK20 OK21 OK25 OK27	OK5 OK9 OK13 OK14 OK18 OK20 OK21 OK22 OK25		OK13 OK14 OK15 OK25 OK35 BK6 BK7 BK8 BK9 BK10 BK11 BK12					OK33 OK34 BK6 BK7 BK8 BK9 BK10 BK11 BK12		
PH-48	OK9 OK13 OK14 OK16 OK17 OK20 OK21 OK23 OK25 OK27 OK35												OK13 OK14 OK15 OK25 OK35 BK6 BK7 BK8 BK9 BK10 BK11 BK12	OK16 OK17 OK20 OK21 OK27 OK35		OK35 BK6 BK7 BK8 BK9 BK10 BK11 BK12		OK33 OK34 BK6 BK7 BK8 BK9 BK10 BK11 BK12	OK5 OK9 OK23	
PH-49	OK9 OK13 OK14 OK16 OK17 OK20 OK21 OK23 OK25 OK27 OK35												OK13 OK14 OK15 OK25 OK35 BK6 BK7 BK8 BK9 BK10 BK11 BK12	OK16 OK17 OK20 OK21 OK27 OK35		OK35 BK6 BK7 BK8 BK9 BK10 BK11 BK12			OK5 OK9 OK23	
PH-50	OK9										OK5		OK13			OK35			OK5	

	ОК13 ОК14 ОК18 ОК20 ОК21 ОК22 ОК23 ОК25 ОК27 ОК35										ОК9 ОК13 ОК14 ОК18 ОК20 ОК21 ОК22 ОК25		ОК14 ОК15 ОК25 ОК35 БК6 БК7 БК8 БК9 БК10 БК11 БК12			БК6 БК7 БК8 БК9 БК10 БК11 БК12			ОК9 ОК23	
РН-51	ОК9 ОК13 ОК14 ОК23 ОК25 ОК27 ОК35												ОК13 ОК14 ОК15 ОК25 ОК35 БК6 БК7 БК8 БК9 БК10 БК11 БК12			ОК35 БК6 БК7 БК8 БК9 БК10 БК11 БК12			ОК5 ОК9 ОК23	
РН-52	ОК9 ОК13 ОК14 ОК16 ОК17 ОК20 ОК21 ОК23 ОК25 ОК27 ОК35												ОК13 ОК14 ОК15 ОК25 ОК35 БК6 БК7 БК8 БК9 БК10 БК11 БК12	ОК16 ОК17 ОК20 ОК21 ОК27 ОК35		ОК35 БК6 БК7 БК8 БК9 БК10 БК11 БК12			ОК5 ОК9 ОК23	
РН-53	ОК9 ОК16 ОК27 ОК33	ОК1 ОК4 ОК11 ОК12 ОК24 ОК30 ОК34 ОК35			ОК12 ОК24 ОК30					ОК8 ОК13 ОК14 ОК17 ОК19 ОК20 ОК21 ОК25	ОК5 ОК9 ОК13 ОК14 ОК18 ОК20 ОК21 ОК22	ОК6 ОК7 ОК8 ОК21 ОК23 ОК26 ОК27 ОК28	ОК13 ОК14 ОК15 ОК25 ОК35 БК6 БК7 БК8	ОК16 ОК17 ОК20 ОК21 ОК27 ОК35		ОК35 БК6 БК7 БК8 БК9 БК10 БК11 БК12			ОК5 ОК9 ОК23	ОК8 ОК20 ОК21 ОК22

		ВК2 ВК3 ВК4 ВК5								ОК27	ОК25	ОК32	ВК9 ВК10 ВК11 ВК12							
РН-54	ОК7 ОК8 ОК9 ОК13 ОК14 ОК16 ОК18 ОК20 ОК22 ОК25 ОК27 ОК28 ОК29 ОК33 ОК35	ОК1 ОК4 ОК11 ОК12 ОК24 ОК30 ОК34 ОК35 ВК2 ВК3 ВК4 ВК5	ОК6 ОК9 ОК13 ОК14 ОК18 ОК21 ОК26 ОК27 ОК28 ОК32 ОК33 ОК34 ОК35 ВК2 ВК3 ВК4 ВК5				ОК3 ОК4 ОК11 ОК12 ОК24 ОК30 ОК33 ОК35 ВК2 ВК3 ВК4 ВК5	ОК3 ОК11 ОК12 ОК30 ОК35 ВК2 ВК3 ВК4 ВК5											

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

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми «Кібербезпека»

Назва структурного/функціонального підрозділу/ Посадова особа	Дата, підпис
1. Навчальний відділ	
2. Відділ забезпечення якості освіти та інноваційного розвитку	
3. Завідувач випускової кафедри	
4. Заступник керівника (проректор з науково-педагогічної роботи)	

РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну програму «Кібербезпека»
бакалаврського (першого) рівня вищої освіти, що запропонована
кафедрою кібербезпеки та інформаційних технологій
Харківського національного економічного університету ім. С. Кузнеця

У сучасному світі важливу роль відіграють інформаційні технології, включно із ними засоби забезпечення кібербезпеки підприємств будь-якої форми власності займають провідні позиції на найвищому рівні із виконанням підприємством своїх безпосередніх бізнес-завдань. Сучасний світ – це технології Індустрії 4.0 та Інтернету речей (як IoT, так і IIoT), де будь-який з фізичних ресурсів підприємства має свою віртуальну копію у цифровій формі, де перехрещуються традиційні підходи до документообігу з інформаційними системами супроводження бізнесу (від PDM до ERP). Це, безумовно, сприяє щорічному збільшенню попиту у нашій країні на спеціалістів з кібербезпеки, які будуть спроможні ефективно вирішувати складні завдання щодо побудови кіберзахисту підприємства та будуть спроможні забезпечувати протидію несанкціонованому втручанню до їх інформаційної інфраструктури.

Освітньо-професійна програма «Кібербезпека» бакалаврського рівня вищої освіти, що запропонована кафедрою кібербезпеки та інформаційних технологій Харківського національного економічного університету ім. С. Кузнеця (ХНЕУ ім. С. Кузнеця), має всі потрібні компоненти щодо забезпечення навчального процесу професійної підготовки фахівців, які у компаніях зможуть займати наступні позиції: менеджера систем з інформаційної безпеки, фахівця захисту інформації, техніка захисту інформації, адміністратору бази даних, адміністратору доступу, інженера-програміста тощо.

Слід визначити, що у сучасних економічних умовах кібербезпека – це не тільки значний тренд у розвитку великих компаній та підприємств. Зараз малий та середній бізнес відкриває нові для себе нові ніші електронної комерції. Відповідно, стає питання щодо забезпечення безперебійної роботи

електронних мереж як корпоративного рівня, так і кіберзахисту в цілому малого та середнього приватного бізнесу. Тому, слід вважати дуже своєчасними завдання, що розглядаються у освітньо-професійній програмі «Кібербезпека», за якою навчаються студенти ХНЕУ ім. С. Кузнеця за спеціальністю 125 «Кібербезпека». Випускник за цією програмою має досвід та розуміння завдань, як у масштабі потреб безпеки як великих організацій та компаній, так і компаній, що мають порівняно невеликі масштаби бізнесу (від середнього аж до мікробізнесу). Запропонована програма враховує потреби як компаній, спрямованих на роботу з закордонними замовниками, так і для компаній, які працюють виключно на внутрішньому ринку України.

Слід підвести, що освітньо-професійна програма «Кібербезпека» бакалаврського (першого) рівня вищої освіти, що запропонована кафедрою кібербезпеки та інформаційних технологій ХНЕУ ім. С. Кузнеця, є сучасною, ефективною та затребуваною на ринку праці нашої країни щодо підготовки фахівців з кібербезпеки. Ця програма відповідає стандарту Міністерства освіти і науки України та узгоджується з запитами компаній роботодавців щодо наявності кваліфікованих кадрів у ІТ-галузі та напряму спеціальності 125 «Кібербезпека».

Ректор
ПЗВО «Харківський технологічний університет «ШАГ», д.т.н., професор
_____ В.Є. Зайцев

«16» вересня 2020 р.

Виконавчий директор
ГС «ХАРКІВСЬКИЙ КЛАСТЕР ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ»
_____ О.С. Шаповал

«16» вересня 2020 р.

IT безпека

РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну програму «Кібербезпека»,
підготовлену кафедрою кібербезпеки та інформаційних технологій
Харківського національного економічного університету
імені Семена Кузнеця

Забезпечення необхідного рівня кібербезпеки бізнес процесів і методів захисту цифрового обладнання, інформації та комп'ютерних систем від навмисного чи несанкціонованого доступу вразливості комп'ютерних та інформаційних систем становлять значну проблему для усіх суб'єктів економічної діяльності сучасної бізнес-спільноти. При інтенсивному розвитку інформаційного оточення яке охоплює майже усі сфери бізнес процесів у економічному просторі суспільства та держави, характеризується величезним збільшенням об'єму даних у які потребують запобігання і нейтралізації реальних і потенційних загроз.

До фахівців з кібербезпеки висуваються досить високі вимоги щодо здійснення професійної діяльності щодо успішного впровадження на ринку праці, тому що сучасним трендом розвитку технологій розробки програмних продуктів є рішення, які надають можливість вирішувати завдання проектування, програмування, влагодження, розгортання, супроводження, забезпечення необхідного рівня кібербезпеки, зберігання даних, організацію хмарних сервісів, які пов'язані підтримкою програмних рішень у корпоративному середовищі.

Кафедрою кібербезпеки та інформаційних технологій Харківського національного економічного університету ім. С. Кузнеця, відповідно до останніх тенденцій розвитку технологій автоматизації бізнес-процесів, економічних завдань та повсякденної економічної діяльності підприємств з урахуванням технологічних можливостей держави та потреб бізнес-спільноти України у межах перспектив цифрової трансформації на державному рівні, розроблено навчальну програму «Кібербезпека», та навчальні плани дисциплін пов'язаних з напрямком підготовки фахівця з інформаційної безпеки широкого профілю, яка повністю реалізує результати навчання передбачені стандартом вищої освіти за спеціальністю 125 Кібербезпека.

Програма дозволяє забезпечити підготовку фахівця здатного забезпечити необхідний рівень кібербезпеки розгалуженої IT інфраструктури у високотехнологічних системах хмарних мереж щодо розробки, впровадження і супроводження програмних та програмно-апаратних комплексів засобів інформаційної безпеки в інформаційно-комунікаційних системах на корпоративному рівні, враховуючи принципи застосування криптографічних методів у блокчейн технологіях відповідно до обмеження та ризиків створення та використання блокчейн платформ в

межах національних і міжнародних, стандартів й практик щодо здійснення професійної діяльності.

Навчальний процес організовано на базі сучасних інтегрованих середовищах розробки корпоративних додатків та систем збереження даних з санкціонованим доступом. Кожному студенту на період навчання безкоштовно надається ліцензований доступ до додатків та сервісів у аккаунті у порталу Microsoft 365.

Вважаємо, що Освітньо-професійна програма «Кібербезпека», що складена та запропонована кафедрою кібербезпеки та інформаційних технологій Харківського національного економічного університету ім. С. Кузнеця, у відповідності до сучасних тенденцій на попит фахівців з кібербезпеки, має всі необхідні компоненти для підготовки кваліфікованих спеціалістів, щодо забезпечення кібербезпеки економічної діяльності підприємств корпоративного рівня, спроможних здійснювати аналіз, проектування програмування, влагодження, розгортання, супроводження, при організації хмарних сервісів використовуючи сучасні технології які надають ліцензійні інтегровані середовища розробки.

Навчання за Освітньо-професійною програмою «Кібербезпека», забезпечує студентам надбання необхідних компетенцій, навичок та спроможностей щодо впровадженням та підтримки програмних рішень у корпоративному середовищі у межах законодавчої нормативно-правової бази та вимог відповідних національних і міжнародних, стандартів щодо здійснення успішної професійної діяльності.

РЕЦЕНЗІЯ
на освітньо-професійну програму Кібербезпека / Cybersecurity
Харківського національного економічного університету імені Семена Кузнеця

Подана на рецензування Харківським національним економічним університетом імені Семена Кузнеця освітньо-професійна програма (ОПП) Кібербезпека / Cybersecurity призначена для здобуття студентами на першому (бакалаврському) рівні освіти ступеня вищої освіти бакалавр. Детальне вивчення ОПП показало, що вона у повній мірі задовольняє вимогам, викладеним в затвердженому і введеному в дію наказом Міністерства освіти і науки України від 04.10.2018 р. № 1047 стандарті 125 – Кібербезпека (бакалаврський рівень).

Однією з позитивних рис ОПП, що рецензується є участь в складі групи розробників не тільки вчених та студентів – представників університету, а й представників відомих в Україні ІТ компаній: ТОВ "Сайфер БІС" та "Distributed Lab". Такий підхід свідчить про принцип нерозривності між освітою та практикою, який закладений в стандарті. Як результат на виході в ОПП вказаний достатньо широкий спектр для працевлаштування випускників – від менеджерів систем з інформаційної безпеки до інженерів-програмістів.

Другою особливістю ОПП є те, що співвідношення між циклом загальної підготовки та циклом професійної підготовки співвідносяться як 12% до 88% з наявних 240 кредитів ЄКТС. Таким чином, можна зробити висновок, що ОПП є більш професійно орієнтована на відміну від більшості схожих програм інших вищих закладів вищої освіти. Поряд з тим, одним з недоліків програми на наш погляд є те, що в програмі непередбачено власних компетентностей та результатів навчання. Використано лише ті, які є в стандарті 125 – Кібербезпека. Іншим недоліком програми є відсутність дисциплін, які в своїй назві містять топонім Кібер.

Серед ключових особливостей ОПП є приведення авторами співвідношень між загальними компетентностями та результатами навчання, що не приведено в стандарті.

Ознайомлюючись з ОПП студенти мають змогу в повній мірі ознайомитися з структурою програми. Крім того студенти мають змогу познайомимся з формами атестації, які на них чекають в ході навчання та тими документами на які є послання в програмі та на яких грунтуються принципи атестації.

Рецензуєма ОПП містить вимоги до системи внутрішнього забезпечення якості вищої освіти, перелік нормативних документів, на яких базується освітньо-професійна програма, а також перелік використаних джерел.

У пояснювальній записці до ОПП авторами подано матрицю відповідності визначених компетентностей дескрипторам національної рамки кваліфікації. Такий підхід, на відміну від інших ОПП описує ключові дескриптори, що забезпечуються у разі набуття відповідних компетентностей. Також додатки містять матриці: відповідності визначених результатів навчання та компетентностей; відповідності освітніх компонентів і компетентностей освітньої програми; відповідності освітніх компонентів і результатів навчання освітньої програми. Наявність таких матриць за своєю суттю є дорожньою картою студента в процесі опанування освітньої програми.

Отже, в цілому можна стверджувати: ОПП, що рецензується є унікальною програмою, яка несхожа з іншими аналогами; програма є професійно орієнтованою; програма є сучасною та такою, що максимально спрямована на працевлаштування майбутніх бакалаврів з кібербезпеки.

Рецензент:
начальник кафедри захисту інформації та кібербезпеки
факультету охорони державної таємниці та інформаційного протиборства
Житомирського військового інституту імені С. П. Корольова
доктор технічних наук (зі спеціальності 21.05.01 – інформаційна безпека держави)
професор (із спеціальності – 125 Кібербезпека)
полковник Руслан ГРИЩУК
"14" вересня 2020 р.

Підпис професора Грищука Р. засвідчую.
ТВО начальника відділу персоналу та стройового Віктор КІСЕЛЬОВ

РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну програму «Кібербезпека»,
підготовлену кафедрою кібербезпеки та інформаційних технологій
Харківського національного економічного університету імені Семена Кузнеця

Сьогодні, у часи цифрового суспільства, вплив інформаційно-комунікаційних технологій на життя людини зростає у геометричній прогресії – виникають нові загрози і нові виклики. Саме тому особливої актуальності дедалі більше набуває поняття «кібербезпека». Якісна підготовка здобувачів вищої освіти в сфері кібербезпеки на теперішній час для України є важливим завданням. Вони покликані захищати ресурси (інформації, комп'ютерів, серверів, підприємств, приватних осіб), а також дані на етапі їх обміну та збереження.

Харківський національний економічний університет імені Семена Кузнеця в цьому питанні має досвід, потужний кадровий потенціал та матеріально-технічну базу для виконання поставленого завдання. Рецензована освітньо-професійна програма «Кібербезпека» розроблена проектною групою працівників кафедри кібербезпеки та інформаційних технологій після консультацій із науковцями, потенційними роботодавцями, які підтвердили потребу підготовки фахівців цієї спеціальності. В освітньо-професійній програмі визначені програмні компетентності виходячи із видів і завдань діяльності кіберзахисту. Вони розподілені на загальні та фахові компетентності, найбільш відповідні для запропонованої програми. Фахові компетентності носять практичний характер і можуть бути використані у професійній діяльності майбутніх фахівців. Навчальний план підготовки бакалаврів освітньо- професійної програми «Кібербезпека» повністю відповідає завданням освітньої професійної програми. Послідовність вивчення дисциплін, план та графік навчального процесу, перелік та обсяг нормативних та вибіркових дисциплін відповідають структурно-логічній схемі підготовки здобувачів вищої освіти за спеціальністю 125 «Кібербезпека» і покликані сприяти забезпеченню відповідності програмних результатів навчання запитам потенційних роботодавців (стейкхолдерів).

ТОВ «ДОСЛІДНИЦЬКО-ТЕХНІЧНИЙ
ОСВІТНІЙ ЦЕНТР «ВОЛЬТ» Богдан ВОРОБЙОВ

РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну програму «Кібербезпека»,
підготовлену кафедрою кібербезпеки та інформаційних технологій
Харківського національного економічного університету імені Семена Кузнеця

Робота сучасних фахівців в різних сферах діяльності, незалежно від посад, які вони обіймають, так, або інакше пов'язана з використанням інформаційних систем. Забезпечення надійної, безперебійної роботи таких інформаційних систем життєво необхідне як на загальнодержавному рівні, так і в умовах повсякденної діяльності окремих підприємств, установ, бізнес компаній, тощо. Не менш важливою функціональною складовою є захист інформації в інформаційних системах від спотворення, викрадення, або несанкціонованого використання. Підтримка та реалізація таких функції є прерогативою фахівців з кібербезпеки, роль яких посилюється, стає дедалі більш актуальною з розвитком високотехнологічного та інформатизованого суспільства.

В освітньо-професійній програмі «Кібербезпека» наголошено на актуальних потребах та основних напрямках розвитку щодо забезпечення кібербезпеки. В освітньо-професійній програмі визначені основні програмні компетентності, які передбачають підготовку фахівців у сфері кібербезпеки. Навчальний план підготовки бакалаврів освітньо-професійної програми «Кібербезпека» відповідає завданням освітньої професійної програми. Фахові компетентності, що передбачені у програмі та результати навчання забезпечують високий рівень професійної підготовки випускників, сприяють широкому діапазону їх професійної діяльності та високій конкурентоспроможності на ринку праці.

Освітньо-професійна програма «Кібербезпека», що складена та запропонована кафедрою кібербезпеки та інформаційних технологій Харківського національного економічного університету ім. С. Кузнеця, дозволяє забезпечити сучасну та якісну фахову підготовку бакалаврів за спеціальністю 125 «Кібербезпека». Освітньо-професійна програма містить в собі усі необхідні структурні та змістові складові, відображає сучасні вимоги до підготовки фахівців у сфері кібербезпеки і відповідає запитам практичного використання.

Голова департаменту ІТ комунікацій
ПП "ВКФ "Харківінтелком" Олеся КИРИЧЕНКО