ПРОЕКТ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

“КІБЕРБЕЗПЕКА”
(назва ОПП /ОНП)

РІВЕНЬ ВИЩОЇ ОСВІТИ	**Другий (магістерський)**
СТУПІНЬ ВИЩОЇ ОСВІТИ	**Магістр**
ГАЛУЗЬ ЗНАНЬ	**12 Інформаційні технології**
СПЕЦІАЛЬНІСТЬ	**125 Кібербезпека**

Харків
2021

ПРОЕКТ

ПРЕАМБУЛА

Розробники ОП (Склад робочої групи) у складі:

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

ОП розроблено/оновлено на підставі:

1. Законодавчих та нормативних актів: Законів України «Про освіту», «Про вищу освіту», Національної рамки кваліфікації, Національного класифікатору України: Класифікатор професій (ДК 003:2010).
2. Проект стандарту вищої освіти 125 “Кібербезпека” другого (магістерського) рівня вищої освіти.
3. Аналізу ринку праці, з урахуванням регіонального контексту.
4. Вивчення вітчизняного та зарубіжного досвіду.
5. Пропозицій роботодавців.
6. Рекомендації після процедур внутрішнього та зовнішнього оцінювання ОП (акредитація НАЗЯВО).

Рецензії-відгуки зовнішніх стейкхолдерів (додаються).

ПРОЕКТ

І. ЗАГАЛЬНА ХАРАКТЕРИСТИКА

Рівень вищої освіти	Другий (магістерський) рівень
Ступінь вищої освіти	Магістр
Галузі знань	12 Інформаційні технології
Спеціальності	125 Кібербезпека
Освітня програма (укр. та англ. мовою)	Кібербезпека / Cybersecurity
Форми здобуття освіти, обсяг освітньої програми в кредитах ЄКТС та терміни навчання	очна (денна) форма – 90 кредитів, один рік 4 місяці; заочна форма – 90 кредитів, один рік 4 місяці.
Наявність акредитації	- організація, яка надала акредитацію програми – Національне агентство із забезпечення якості вищої освіти; - сертифікат про акредитацію – № 957 від 18.12.2020 р.; - термін дії акредитації – до 01.07.2026 р.
Мова(и) навчання / оцінювання	українська / англійська
Структурний підрозділ відповідальний за ОП	Кафедра кібербезпеки та інформаційних технологій; Навчальна лабораторія кафедри кібербезпеки та інформаційних технологій
Вимоги до зарахування	(згідно правил прийому)
Обмеження щодо форм навчання	Не має
Освітня кваліфікація	Магістр з кібербезпеки
Кваліфікація(-ї) професійна(-і)	Відсутня
Кваліфікація в дипломі	Ступінь вищої освіти − Магістр Спеціальність – 125 Кібербезпека Освітня програма – Кібербезпека
Мета освітньої програми	підготовка фахівців, здатних розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки, використовувати і впроваджувати технології та застосовувати засоби захисту в системах безпеки контуру бізнес-процесів.
Фокус та особливості (унікальність) програми	Особливостями програми є формування у здобувачів навичок побудови комплексних систем захисту інформації для забезпечення безпеки контуру бізнес-процесів на основі сучасних технологій та програмних застосунків, в умовах розвитку цифрової економіки.

Опис предметної області	**Об'єкти вивчення:** – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; - інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. **Цілі навчання:** Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області** Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. **Методи, методики та технології** Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. **Інструменти та обладнання.** Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.

Академічна мобільність	Польсько-українська програма обміну та двох дипломів для підготовки магістрів за спеціальністю “Кібербезпека” з Університетом у Бєльсько-Бялій (м. Бельсько-Бяла, Польща).
Академічні права	Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.
Професійні права	**Знання і розуміння:** – здатність аналізувати причини та наслідки збоїв або відмов функціонування інформаційних систем, що викликані реалізацією різного класу кіберінцидентів; – здатність розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, а також систему аудиту і контролю функціонування інформаційно-комунікаційних систем та технологій; – здатність розробляти, впроваджувати і супроводжувати системи аудиту та моніторингу якості бізнес/операційних процесів інформаційно-комунікаційних систем та технологій; – здатність розробляти й впроваджувати методи і заходи відновлення штатного функціонування інфраструктури організації в цілому; – здатністьздійснювати процедури управління, контролю та розслідування, надавати рекомендації щодо попередження та аналізу кіберінцидентів; – здатність розробляти стратегію та політику інформаційної безпеки та/або кібербезпеки організації. **Застосування знань і розумінь:** – здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки ; – здатність розробляти, впроваджувати і супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних системах; – здатність розробляти й впроваджувати систему менеджменту інформаційної безпеки та/або кібербезпеки організації; – здатність до проектування, впровадження, супроводження інформаційних мереж і ресурсів, безпеки інформаційних технологій (в т.ч. хмарних технологій та додатків); – здатність розробляти та впроваджувати систему управління інформаційними активами,володіти методами теорії ризик менеджменту та процесних моделей, розробляти моделі загроз й моделі порушника; – здатність розробляти та впроваджувати методи і заходи протидії кіберінцидентам; – здатність розробляти, впроваджувати, та супроводжувати бізнес/операційні процеси з використанням методів та засобів криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. **Формування суджень:** – здатність до пошуку, оброблення та аналізу інформації; – здатність застосовувати знання у практичних ситуаціях; – вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням; – здатність до роботи в команді; – здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпека та/або кібербезпеки.

Працевлаштування випускників	Фахівці з кібербезпеки можуть працювати, згідно з чинною редакцією Національного класифікатора України: Класифікатор професій (ДК 003:2010), а саме: – керівними працівниками апарату місцевих органів державної влади; – керівниками підрозділів комп'ютерних послуг; – керівниками проектів та програм; – менеджерами (управителями) систем з інформаційної безпеки; – розробниками комп'ютерних програм; – викладачами університетів та вищих навчальних закладів; – науковими співробітниками (інформаційна аналітика); – професіоналами в галузі інформації та інформаційні аналітики; – науковими співробітниками (електроніка, телекомунікації); – інженерами в галузі електроніки та телекомунікацій; – науковими співробітниками (проекти та програми); професіоналами з управління проектами та програмами.

ІІ – ПЕРЕЛІК КОМПЕТЕНТНОСТЕЙ ВИПУСКНИКА

Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності	КЗ-1. Здатність застосовувати знання у практичних ситуаціях. КЗ-2. Здатність проводити дослідження на відповідному рівні. КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Фахові компетентності	КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

	КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки 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

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

IV. СТРУКТУРА ОСВІТНЬОЇ ПРОГРАМИ ПІДГОТОВКИ БАКАЛАВРІВ / МАГІСТРІВ / ДОКТОРІВ ФІЛОСОФІЇ

4.1. СТРУКТУРА ПРОГРАМИ ТА ОСВІТНІ КОМПОНЕНТИ

№	Освітні компоненти (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кредити ЄКТС	Структура, %
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
1	*ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ*	13	14
2	*ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ*	20	22
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
3	*ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ*	54	60
4	*ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ*	3	4
	ЗАГАЛЬНА КІЛЬКІСТЬ :	***90***	***100%***
	в тому числі: вибіркова складова		

Код ОК	Освітні компоненти (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кредити ЄКТС	Форми підсумкового контролю
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ			
ЗЦ1	ГОСПОДАРСЬКЕ ПРАВО	2	Залік
ЗЦ2	АНГЛІЙСЬКА МОВА	3	Залік
ЗЦ3	ПРЕЗЕНТАЦІЯ ТА ОБРОБКА ЗНАНЬ	3	Залік
ЗЦ4	МИСТЕЦТВО РЕДАГУВАННЯ ТА РИТОРИКА	2	Залік
ЗЦ5	ЗАХИСТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ	3	Залік
	ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ		
ММ 1	МАГ-МАЙНОР	5	Залік
ММ 2	МАГ-МАЙНОР	5	Залік
ММ 3	МАГ-МАЙНОР	5	Залік

ММ 4	МАГ-МАЙНОР	5	Залік
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ			
ПЦ1	ТЕХНОЛОГІЇ УПРАВЛІННЯ БЕЗПЕКОЮ БІЗНЕС-ПРОЦЕСІВ	3	Залік
ПЦ2	РОЗШИРЕНА МЕРЕЖЕВА ТА ХМАРНА БЕЗПЕКА	3	Екзамен
ПЦ3	ЦИФРОВА КРИМІНАЛІСТИКА	4	Екзамен
ПЦ4	ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ТА ЕТИЧНИЙ ХАКІНГ	4	Екзамен
ПЦ5	ВЕБ-БЕЗПЕКА	3	Екзамен
ПЦ6	БЕЗДРОТОВА ТА МОБІЛЬНА БЕЗПЕКА	4	Екзамен
ПЦ7	ПЕРЕДОВІ МЕТОДИКИ ПРОГРАМУВАННЯ	3	Екзамен
ПЦ8	ПЕРЕДДИПЛОМНА ПРАКТИКА	12	Звіт
ПЦ9	ДИПЛОМНИЙ ПРОЕКТ	18	Дипломний проект
ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ			
ЗЦВ1	КОМПЛЕКСНИЙ ТРЕНІНГ “БЛОКЧЕЙН: МАТЕМАТИЧНІ ПРОБЛЕМИ ТА ЗАСТОСУНКИ” або “КРИПТОГРАФІЯ ТА КРИПТОАНАЛІЗ”	3	Звіт

4.2. ВИБІРКОВА СКЛАДОВА ОСВІТНЬО-ПРОФЕСІЙНОЇ / НАУКОВОЇ ПРОГРАМИ

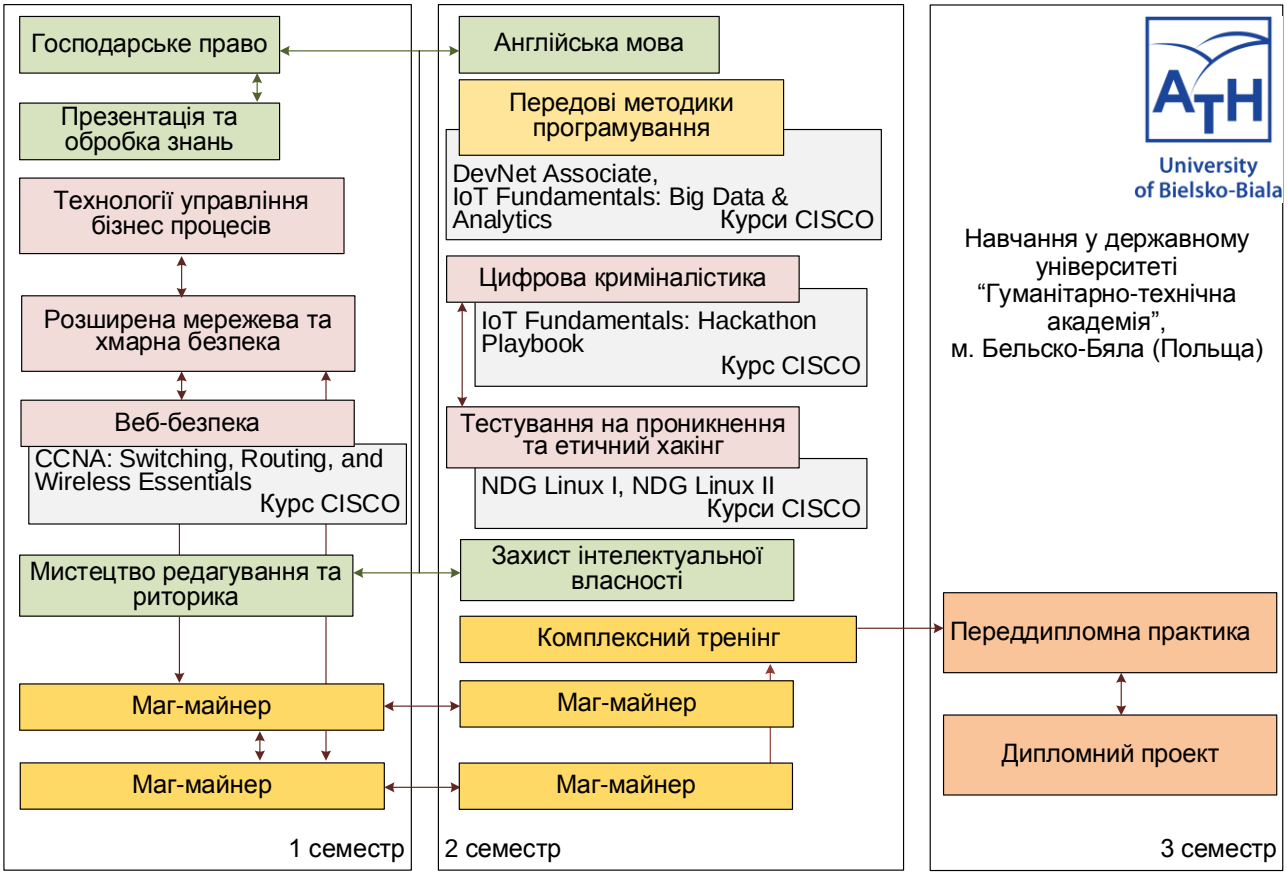
Вибіркова складова освітньо-професійної програми складається з: МАГ-МАЙНОР – умовна назва вибіркових дисциплін із загального переліку Університету (загально-університетський пул) для освітньо-кваліфікаційного рівня магістр. Дисципліни МАГ-МАЙНОР є обов’язковими для вибору здобувачами вищої освіти і входять до загального обсягу кредитів ЄКТС за освітньо-професійною програмою підготовки магістрів.

Ідея дисциплін МАГ-МАЙНОР полягає у вільному виборі здобувачами вищої освіти магістратури дисциплін таких напрямків, які відображають його інтереси, вподобання та плани на майбутнє працевлаштування. Взяти участь у МАГ-МАЙНОР можуть усі факультети і кафедри університету. Індивідуальний план студента буде формуватися з найкращих на його думку навчальних дисциплін.

Загальний обсяг МАГ-МАЙНОР складає 20 кредитів ЄКТС (по 5 кредитів на дисципліну):

КОМПЛЕКСНИЙ ТРЕНІНГ. Головною метою комплексного тренінгу є формування у здобувачів вищої освіти навичок прийняття послідовних рішень щодо вибору механізмів забезпечення безпеки в децентралізованих системах на основі використання блокчейн-технології або методів криптоаналізу щодо визначення рівня стійкості обраних криптосистем.

4.3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ



V. ФОРМИ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи (за наявності)	Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Кваліфікаційна робота має бути розміщена на офіційному сайті (або у репозитарії) закладу вищої освіти або його підрозділу. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.
Вимоги до публічного захисту (за наявності)	У процесі публічного захисту кандидат на присвоєння магістерського 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

Вимоги до системи внутрішнього забезпечення якості в Університеті розроблені на підставі Європейських стандартів та рекомендацій щодо забезпечення якості вищої освіти (ESG), статті 16 Закону України "Про вищу освіту", Стандарту вищої освіти за спеціальністю 125 Кібербезпека другий (магістерський) рівень вищої освіти.

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.
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	Педагогічні і науково-педагогічні працівники Університету можуть підвищувати кваліфікацію за різними формами,

педагогічних, наукових і науково-педагогічних працівників	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 кваліфікації	Достовірна, об'єктивна, актуальна, своєчасна та легкодоступна інформація за освітньо-професійною програмою «Кібербезпека» публікується на сайті ХНЕУ ім. С. Кузнеця, включаючи програми для потенційних

	здобувачів вищої освіти, студентів, випускників, інших стейкхолдерів і громадськості. Публічною є інформація про освітню діяльність за спеціальністю 125 «Кібербезпека», освітньо-професійну програму «Кібербезпека», включаючи критерії відбору на навчання; заплановані результати навчання за цією програмою; процедури навчання, викладання та оцінювання, що використовуються; тощо.
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.

Спеціальні вимоги до зарахування:

Прийом на освітньо-професійну програму «Кібербезпека» Харківського національного економічного університету імені Семена Кузнеця другого (магістерського) рівня вищої освіти здійснюється на конкурсній основі за відповідними джерелами фінансування за умови складання: єдиного вступного іспиту з іноземної мови та фахового вступного випробування, складених в рік вступу.

Конкурсний бал складається з:

оцінка єдиного вступного іспиту з іноземної мови (за шкалою від 100 до 200 балів), мінімальна кількість балів, з якими вступник допускається до участі у конкурсі – 100 балів.

оцінка фахового вступного випробування (за шкалою від 100 до 200 балів), мінімальна кількість балів, з якими вступник допускається до участі у конкурсі – 100 балів.

середній бал документа про здобутий освітній (освітньо-кваліфікаційний рівень) на основі якого здійснюється вступ (за шкалою від 5 до 20 балів) з округленням до сотих частин бала. Мінімальна кількість балів, з якими вступник допускається до участі у конкурсі – 5 балів.

Для успішного засвоєння освітньо-професійної програми магістра абітурієнти повинні мати перший (бакалаврський) рівень вищої освіти (диплом бакалавра), підтверджений документом державного зразка, що виданий закладом вищої освіти III–IV рівня акредитації.

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

Код КП	Професійна назва роботи
1236	Керівники підрозділів комп'ютерних послуг
1238	Керівники проектів та програм
1495	Менеджери (управителі) систем з інформаційної безпеки
2132.2	Розробники комп'ютерних програм
2433.1	Наукові співробітники (інформаційна аналітика)
2433.2	Професіонали в галузі інформації та інформаційні аналітики
2447.1	Наукові співробітники (проекти та програми)
1229.3	Керівні працівники апарату місцевих органів державної влади;
231	Викладачі університетів та вищих навчальних закладів;
2144.1	Наукові співробітники (електроніка, телекомунікації);
2144.2	Інженери в галузі електроніки та телекомунікацій;
2447.2	Професіонали з управління проектами та програмами.

ПРОЕКТ

ПОЯСНЮВАЛЬНА ЗАПИСКА

Матриця відповідності визначених Стандартом (за наявності) компетентностей дескрипторам НРК та матриця відповідності визначених Стандартом результатів навчання та компетентностей представлені в Таблицях 1 і 2.

Таблиця 1

Матриця відповідності визначених Стандартом компетентностей / результатів навчання дескрипторам НРК

Класифікація компетентностей (результатів навчання) за НРК	**Знання Зн1** Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основою для оригінального мислення та проведення досліджень **Зн2** Критичне осмислення проблем у галузі та на межі галузей знань	**Уміння/Навички Ум1** Спеціалізовані уміння/навички розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур **Ум2** Здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах **Ум3** Здатність розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності	**Комунікація К1** Зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і нефахівців, зокрема до осіб, які навчаються	**Відповідальність і автономія АВ1** Управління робочими або навчальними процесами, які є складними, непередбачуваними та потребують нових стратегічних підходів **АВ2** Відповідальність за внесок до професійних знань і практики та/або оцінювання результатів діяльності команд та колективів **АВ3** Здатність продовжувати навчання з високим ступенем автономії
Загальні компетентності				
КЗ1	Зн1, Зн2	Ум1, Ум3	К1	АВ1, АВ2
КЗ2	Зн1, Зн2	Ум1, Ум2, Ум3		АВ2, АВ3
КЗ3	Зн2	Ум2, Ум3		АВ1
КЗ4	Зн1	Ум3		АВ1, АВ2
КЗ5	Зн2	Ум2	К1	АВ1
Спеціальні (фахові) компетентності				
КФ1	Зн1	Ум2		АВ2
КФ2	Зн1, Зн2	Ум2		АВ2
КФ3	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2

Класифікація компетентностей (результатів навчання) за НРК	**Знання Зн1** Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основою для оригінального мислення та проведення досліджень **Зн2** Критичне осмислення проблем у галузі та на межі галузей знань	**Уміння/Навички Ум1** Спеціалізовані уміння/навички розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур **Ум2** Здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах **Ум3** Здатність розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності	**Комунікація К1** Зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і нефахівців, зокрема до осіб, які навчаються	**Відповідальність і автономія АВ1** Управління робочими або навчальними процесами, які є складними, непередбачуваними та потребують нових стратегічних підходів **АВ2** Відповідальність за внесок до професійних знань і практики та/або оцінювання результатів діяльності команд та колективів **АВ3** Здатність продовжувати навчання з високим ступенем автономії
КФ4	Зн1, Зн2	Ум1, Ум2	К1	АВ1, АВ2
КФ5	Зн1, Зн2	Ум1, Ум2	К1	АВ1, АВ2
КФ6	Зн1	Ум1, Ум2	К1	АВ1
КФ7	Зн1	Ум1, Ум2	К1	АВ1
КФ8	Зн1	Ум1, Ум2	К1	АВ1
КФ9	Зн1	Ум1, Ум2	К1	АВ1
КФ10	Зн2	Ум1, Ум2, Ум3	К1	АВ1, АВ2

Таблиця 2

Матриця відповідності визначених результатів навчання, компетентностей та освітніх компонентів

Програмні результати навчання	**Компетентності**															
	Загальні					**Спеціальні (фахові)**										
	КЗ1	**КЗ2**	**КЗ3**	**КЗ4**	**КЗ5**	**КФ1**	**КФ2**	**КФ3**	**КФ4**	**КФ5**	**КФ6**	**КФ7**	**КФ8**	**КФ9**	**КФ10**	**КФ11**
РН 1	ОК13 ОК14		ОК5 ОК7			ОК7 ОК10 ОК11 ОК12										
РН 2		ОК3 ОК12 ОК13	ОК5 ОК7			ОК7 ОК10 ОК11 ОК12	ОК1 ОК5 ОК6	ОК6 ОК8 ОК9 ОК10								
РН 3	ОК13 ОК14					ОК7 ОК10 ОК11 ОК12										
РН 4	ОК13 ОК14	ОК3 ОК12 ОК13	ОК5 ОК7	ОК5 ОК13		ОК7 ОК10 ОК11 ОК12	ОК1 ОК5 ОК6									
РН 5			ОК5 ОК7		ОК4	ОК2	ОК1 ОК5 ОК6									
РН 6	ОК13 ОК14			ОК13		ОК7 ОК10 ОК11 ОК12		ОК6 ОК8 ОК9 ОК10		ОК7 ОК8 ОК9 ОК10	ОК6 ОК7 ОК10 ОК11	ОК8 ОК9		ОК6		
РН 7	ОК13 ОК14		ОК5 ОК7				ОК1 ОК5 ОК6									
РН 8	ОК13 ОК14	ОК3 ОК12 ОК13		ОК5 ОК13	ОК4	ОК2		ОК6 ОК8 ОК9 ОК10						ОК6	ОК4	
РН 9	ОК13 ОК14	ОК3 ОК12	ОК5 ОК7	ОК5 ОК13					ОК6 ОК7					ОК6		

ПРОЕКТ

Програмні результати навчання	Компетентності															
	Загальні					Спеціальні (фахові)										
	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11
		ОК13														
РН 10	ОК13 ОК14		ОК5 ОК7	ОК5 ОК13						ОК7 ОК8 ОК9 ОК10				ОК6		
РН 11	ОК13 ОК14		ОК5 ОК7	ОК5 ОК13							ОК6 ОК7 ОК10 ОК11				ОК4	
РН 12	ОК13 ОК14		ОК5 ОК7	ОК5 ОК13					ОК6 ОК7			ОК8 ОК9			ОК4	
РН 13	ОК13 ОК14		ОК5 ОК7	ОК5 ОК13									ОК7 ОК10 ОК11		ОК4	
РН 14	ОК13 ОК14		ОК5 ОК7	ОК5 ОК13					ОК6 ОК7					ОК6	ОК4	
РН 15				ОК5 ОК13	ОК4	ОК2									ОК4	
РН 16	ОК13 ОК14	ОК3 ОК12 ОК13	ОК5 ОК7	ОК5 ОК13				ОК6 ОК8 ОК9 ОК10	ОК6 ОК7	ОК7 ОК8 ОК9 ОК10	ОК6 ОК7 ОК10 ОК11	ОК8 ОК9		ОК6	ОК4	
РН 17								ОК6 ОК8 ОК9 ОК10							ОК4	
РН 18	ОК13 ОК14			ОК5 ОК13	ОК4	ОК2									ОК4	
РН 19	ОК13 ОК14			ОК5 ОК13	ОК4	ОК2 ОК7 ОК10 ОК11 ОК12	ОК1 ОК5 ОК6	ОК6 ОК8 ОК9 ОК10	ОК6 ОК7		ОК6 ОК7 ОК10 ОК11	ОК8 ОК9	ОК7 ОК10 ОК11	ОК6		

ПРОЕКТ

Програмні результати навчання	Компетентності															
	Загальні					Спеціальні (фахові)										
	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11
РН 20	ОК13 ОК14	ОК3 ОК12 ОК13	ОК5 ОК7	ОК5 ОК13	ОК4	ОК2 ОК7 ОК10 ОК11 ОК12		ОК6 ОК8 ОК9 ОК10								
РН 21	ОК13 ОК14	ОК3 ОК12 ОК13	ОК5 ОК7	ОК5 ОК13		ОК7 ОК10 ОК11 ОК12		ОК6 ОК8 ОК9 ОК10		ОК7 ОК8 ОК9 ОК10		ОК8 ОК9	ОК7 ОК10 ОК11			
РН 22		ОК3 ОК12 ОК13	ОК5 ОК7	ОК5 ОК13		ОК7 ОК10 ОК11 ОК12		ОК6 ОК8 ОК9 ОК10								
РН 23	ОК13 ОК14		ОК5 ОК7	ОК5 ОК13		ОК7 ОК10 ОК11 ОК12	ОК1 ОК5 ОК6	ОК6 ОК8 ОК9 ОК10			ОК6 ОК7 ОК10 ОК11	ОК8 ОК9	ОК7 ОК10 ОК11	ОК6		

Гарант ОП **_____** **Мілов О.В.**
професор кафедри кібербезпеки
та інформаційних технологій, д.т.н., проф.