

**ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«КІБЕРБЕЗПЕКА»**

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

ПРЕАМБУЛА

Розробники ОП (Склад робочої групи) у складі:

1. Мілов Олександр Володимирович – доктор технічних наук, професор, професор кафедри кібербезпеки та інформаційних технологій.
2. Євсєєв 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.

Розглянуто на засіданні кафедри кібербезпеки та інформаційних технологій

Розглянуто вченою радою факультету інформаційних технологій

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).

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	<p>Об'єкти вивчення:</p> <ul style="list-style-type: none"> – 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. <p>Цілі навчання: Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки.</p> <p>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.</p> <p>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</p>

	<p>професійних задач в галузі інформаційної безпеки та/або кібербезпеки.</p> <p>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.</p> <p>Інструменти та обладнання.</p> <p>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.</p>
<p>Академічна мобільність</p>	<p>Польсько-українська програма обміну та двох дипломів для підготовки магістрів за спеціальністю “Кібербезпека” з Університетом у Бельсько-Бялій (м. Бельсько-Бяла, Польща).</p>
<p>Академічні права</p>	<p>Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти.</p> <p>Набуття додаткових кваліфікацій в системі освіти дорослих.</p>
<p>Професійні права</p>	<p>Знання і розуміння:</p> <ul style="list-style-type: none"> – 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; – здатність здійснювати процедури управління, контролю та розслідування, надавати рекомендації щодо попередження та аналізу кіберінцидентів; – здатність розробляти стратегію та політику інформаційної безпеки та/або кібербезпеки організації. <p>Застосування знань і розуміння:</p> <ul style="list-style-type: none"> – 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

	<p>інформаційної безпеки та/або кібербезпеки організації;</p> <ul style="list-style-type: none"> – 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. <p>Формування суджень:</p> <ul style="list-style-type: none"> – 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 безпеки та/або кібербезпеки.
<p>Працевлаштування випускників</p>	<p>Фахівці з кібербезпеки можуть працювати, згідно з чинною редакцією Національного класифікатора України: Класифікатор професій (ДК 003:2010), а саме:</p> <ul style="list-style-type: none"> – 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; – професіоналами в галузі інформації та інформаційні аналітики; – інженерами в галузі електроніки та телекомунікацій; – професіоналами з управління проектами та програмами.

II – ПЕРЕЛІК КОМПЕТЕНТНОСТЕЙ ВИПУСКНИКА

<p>Інтегральна компетентність</p>	<p>Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.</p>
<p>Загальні компетентності</p>	<p>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</p>

	<p>професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).</p>
<p>Фахові компетентності</p>	<p>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.</p> <p>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.</p> <p>КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.</p> <p>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.</p> <p>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.</p> <p>КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.</p> <p>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.</p> <p>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.</p> <p>КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування</p>

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**).

III – 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.

PH7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

PH8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

PH9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

PH10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

PH11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

PH12. 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.

PH13. 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.

PH14. 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.

PH15. 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.

PH16. 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.

PH17. 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.

PH18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та/або кібербезпеки.

PH19. 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.

PH20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

PH21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

PH22. 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.

PH23. 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	<i>ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ</i>	13	115
2	<i>ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ</i>	20	22
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
3	<i>ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ</i>	54	60
4	<i>ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ</i>	3	3
ЗАГАЛЬНА КІЛЬКІСТЬ :		90	100%
<i>в тому числі: вибіркова складова</i>		23	25%

Код ОК	Освітні компоненти (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кредити ЄКТС	Форми підсумкового контролю
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
<i>ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ</i>			
ОК1	ГОСПОДАРСЬКЕ ПРАВО	2	Залік
ОК2	АНГЛІЙСЬКА МОВА	3	Залік
ОК3	ПРЕЗЕНТАЦІЯ ТА ОБРОБКА ЗНАНЬ	3	Залік
ОК4	МИСТЕЦТВО РЕДАГУВАННЯ ТА РИТОРИКА	2	Залік
ОК5	ЗАХИСТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ	3	Залік
<i>ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ</i>			
ВК1	МАГ-МАЙНОР	5	Залік
ВК2	МАГ-МАЙНОР	5	Залік
ВК3	МАГ-МАЙНОР	5	Залік

ВК4	МАГ-МАЙНОР	5	Залік
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
<i>ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ</i>			
ОК6	ТЕХНОЛОГІЇ УПРАВЛІННЯ БЕЗПЕКОЮ БІЗНЕС-ПРОЦЕСІВ	3	Залік
ОК7	РОЗШИРЕНА МЕРЕЖЕВА ТА ХМАРНА БЕЗПЕКА	3	Екзамен
ОК8	ЦИФРОВА КРИМІНАЛІСТИКА	4	Екзамен
ОК9	ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ТА ЕТИЧНИЙ ХАКІНГ	4	Екзамен
ОК10	ВЕБ-БЕЗПЕКА	3	Екзамен
ОК11	БЕЗДРОТОВА ТА МОБІЛЬНА БЕЗПЕКА	4	Екзамен
ОК12	ПЕРЕДОВІ МЕТОДИКИ ПРОГРАМУВАННЯ	3	Екзамен
ОК13	ПЕРЕДДИПЛОМНА ПРАКТИКА	15	Звіт
ОК14	ДИПЛОМНИЙ ПРОЕКТ	15	Дипломний проект
<i>ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ</i>			
ВК5	КОМПЛЕКСНИЙ ТРЕНІНГ “БЛОКЧЕЙН: МАТЕМАТИЧНІ ПРОБЛЕМИ ТА ЗАСТОСУНКИ	3	Звіт

4.2. ВИБІРКОВА СКЛАДОВА ОСВІТНЬО-ПРОФЕСІЙНОЇ

Вибіркова складова навчального плану освітньої програми складається з: МАГ-МАЙНОРІВ, КОМПЛЕКСНОГО ТРЕНІНГУ.

МАГ-МАЙНОР – умовна назва вибіркового навчального дисциплін підготовки освітнього ступеня магістр (МАЙНОР для магістрів). Сутність МАГ-МАЙНОРІВ полягає у вільному виборі навчальних дисциплін таких напрямків, які відображають інтереси здобувачів вищої освіти, їх вподобання та плани на майбутнє працевлаштування. МАГ-МАЙНОР є обов'язковою складовою освітніх програм

Обсяг дисципліни МАГ-МАЙНОР – складає 5 кредитів ЄКТС. Формою підсумкового контролю є залік. Загальний обсяг дисциплін маг-майнорів складає 20 кредитів ЄКТС.

Здобувачі вищої освіти очної (денної) форми навчання обирають по дві дисципліни в 1 та 2 семестрі на першому році навчання.

Здобувачі вищої освіти заочної форми навчання обирають 4 дисципліни на 2 році навчання.

КОМПЛЕКСНИЙ ТРЕНІНГ – тренінг, що обирають здобувачі вищої освіти другого (магістерського) рівня. Тренінг спрямований на отримання здобувачами вищої освіти практичних, комунікативних навичок.

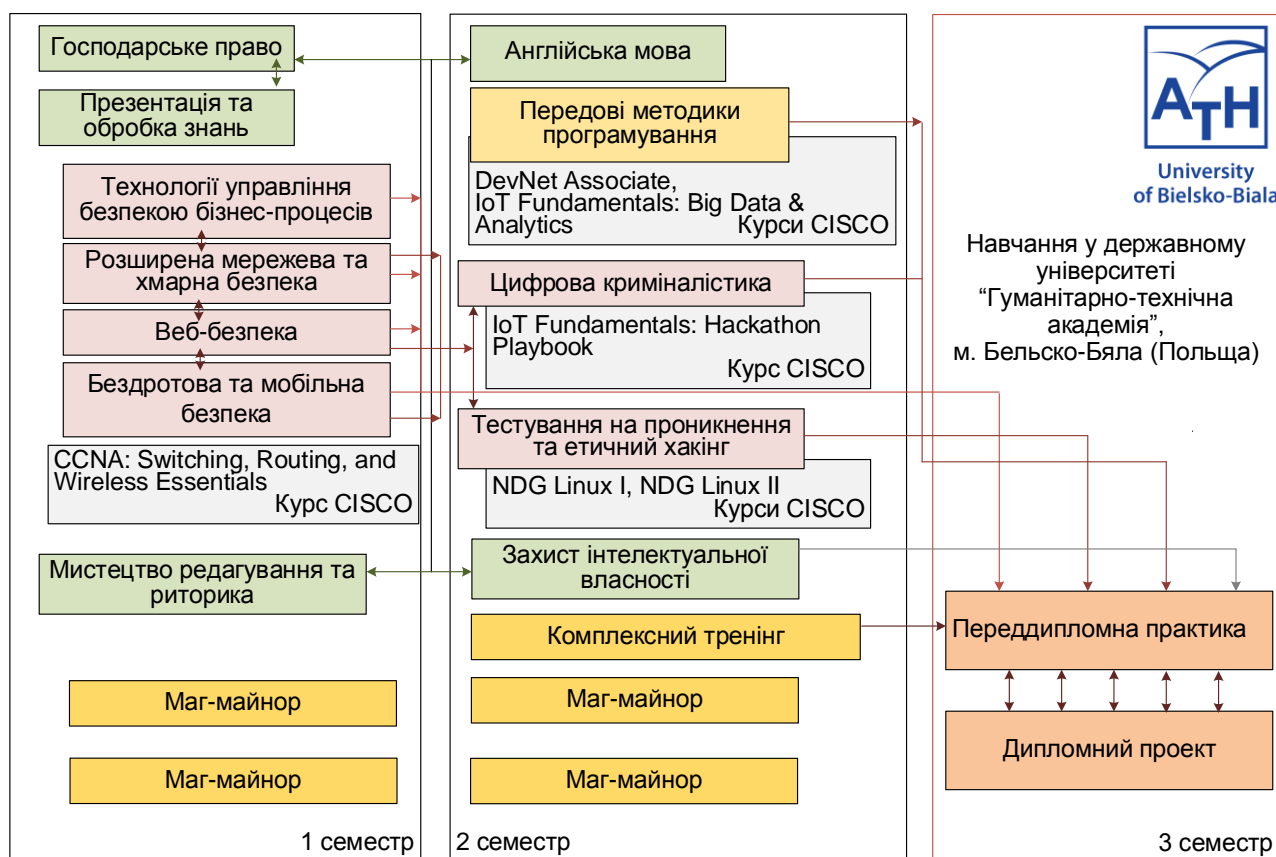
Комплексний тренінг здобувачі вищої освіти обирають на першому або другому році навчання залежно від спеціальності (освітньої програми).

Обсяг комплексного тренінгу складає 3 кредити ЄКТС. За результатами комплексного тренінгу формується звіт.

Вибіркові навчальні дисципліни не формують результати навчання, що передбачені стандартом вищої освіти для відповідного рівня, але можуть поглиблювати певні з них та розвивати софтскілс.

Здобувачі вищої освіти заочної форми навчання обирають 4 дисципліни на 1 або 2 році навчання залежно від спеціальності (освітньої програми).

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	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	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.

Політика щодо 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; забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації; забезпечення дотримання академічної доброчесності працівниками закладів вищої освіти та здобувачами вищої
---	--

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

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

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

Матриця відповідності визначених 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

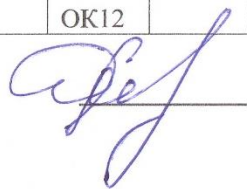
Матриця відповідності визначених результатів навчання, компетентностей та освітніх компонентів

Програмні результати навчання	Компетентності															
	Загальні					Спеціальні (фахові)										
	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11
PH 1	OK13 OK14		OK5 OK7			OK7 OK10 OK11 OK12										
PH 2		OK3 OK12 OK13	OK5 OK7			OK7 OK10 OK11 OK12	OK1 OK5 OK6	OK6 OK8 OK9 OK10								
PH 3	OK13 OK14					OK7 OK10 OK11 OK12										
PH 4	OK13 OK14	OK3 OK12 OK13	OK5 OK7	OK5 OK13		OK7 OK10 OK11 OK12	OK1 OK5 OK6									
PH 5			OK5 OK7		OK4	OK2	OK1 OK5 OK6									
PH 6	OK13 OK14			OK13		OK7 OK10 OK11 OK12		OK6 OK8 OK9 OK10		OK7 OK8 OK9 OK10	OK6 OK7 OK10 OK11	OK8 OK9		OK6		
PH 7	OK13 OK14		OK5 OK7				OK1 OK5 OK6									
PH 8	OK13 OK14	OK3 OK12		OK5 OK13	OK4	OK2		OK6 OK8						OK6	OK4	

Програмні результати навчання	Компетентності															
	Загальні					Спеціальні (фахові)										
	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11
		OK13						OK9 OK10								
PH 9	OK13 OK14	OK3 OK12 OK13	OK5 OK7	OK5 OK13					OK6 OK7					OK6		
PH 10	OK13 OK14		OK5 OK7	OK5 OK13						OK7 OK8 OK9 OK10				OK6		
PH 11	OK13 OK14		OK5 OK7	OK5 OK13							OK6 OK7 OK10 OK11				OK4	
PH 12	OK13 OK14		OK5 OK7	OK5 OK13					OK6 OK7			OK8 OK9			OK4	
PH 13	OK13 OK14		OK5 OK7	OK5 OK13									OK7 OK10 OK11		OK4	
PH 14	OK13 OK14		OK5 OK7	OK5 OK13					OK6 OK7					OK6	OK4	
PH 15				OK5 OK13	OK4	OK2									OK4	
PH 16	OK13 OK14	OK3 OK12 OK13	OK5 OK7	OK5 OK13				OK6 OK8 OK9 OK10	OK6 OK7	OK7 OK8 OK9 OK10	OK6 OK7 OK10 OK11	OK8 OK9		OK6	OK4	
PH 17								OK6 OK8 OK9 OK10							OK4	
PH 18	OK13 OK14			OK5 OK13	OK4	OK2									OK4	
PH 19	OK13			OK5	OK4	OK2	OK1	OK6	OK6		OK6	OK8	OK7	OK6		

Програмні результати навчання	Компетентності															
	Загальні					Спеціальні (фахові)										
	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11
	OK14			OK13		OK7 OK10 OK11 OK12	OK5 OK6	OK8 OK9 OK10	OK7		OK7 OK10 OK11	OK9	OK10 OK11			
PH 20	OK13 OK14	OK3 OK12 OK13	OK5 OK7	OK5 OK13	OK4	OK2 OK7 OK10 OK11 OK12		OK6 OK8 OK9 OK10								
PH 21	OK13 OK14	OK3 OK12 OK13	OK5 OK7	OK5 OK13		OK7 OK10 OK11 OK12		OK6 OK8 OK9 OK10		OK7 OK8 OK9 OK10		OK8 OK9	OK7 OK10 OK11			
PH 22		OK3 OK12 OK13	OK5 OK7	OK5 OK13		OK7 OK10 OK11 OK12		OK6 OK8 OK9 OK10								
PH 23	OK13 OK14		OK5 OK7	OK5 OK13		OK7 OK10 OK11 OK12	OK1 OK5 OK6	OK6 OK8 OK9 OK10			OK6 OK7 OK10 OK11	OK8 OK9	OK7 OK10 OK11	OK6		

Гарант ОП



Мілов О.В.
професор кафедри кібербезпеки
та інформаційних технологій, д.т.н., проф.