МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖЕНО
Ректор ВНТУ
_____ Віктор БІЛІЧЕНКО
Наказ ВНТУ №20 від 26.01.2023

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

Безпека інформаційних і комунікаційних систем
Information and Communications Systems Security

Рівень вищої освіти	другий (магістерський)
Спеціальність	125 Кібербезпека та захист інформації
Галузь знань	12 Інформаційні технології
Освітня кваліфікація	магістр з кібербезпеки та захисту інформації

Розглянуто та схвалено
на засіданні Вченої Ради ВНТУ
Протокол № 6 від 26.01.2023

Вінниця, 2023

ЛИСТ ПОГОДЖЕННЯ

ОПП Безпека інформаційних і комунікаційних систем

Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека та захист інформації

Гарант ОПП
к.т.н., доцент, доцент кафедри ЗІ _____ Олеся ВОЙТОВИЧ

Директор Центру забезпечення
якості освіти ВНТУ _____ Олеся ВОЙТОВИЧ

Освітньо-професійну програму розглянуто та схвалено на засіданні кафедри захисту інформації;

протокол № 6 від 17 грудня 2022 р.

Зав. кафедри _____ Володимир ЛУЖЕЦЬКИЙ

ОПП розглянуто після надходження всіх зауважень та пропозицій та схвалено на:

засіданні Вченої ради факультету інформаційних технологій та комп'ютерної інженерії;
протокол №5 від 17 січня 2023 р.

Голова _____ Світлана КИРИЛАЩУК

засіданні Методичної ради ВНТУ,
протокол №6 від 19 січня 2023 р.

Голова _____ Олександр Петров

ПРЕАМБУЛА

ОПП Безпека інформаційних і комунікаційних систем

Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека та захист інформації

РОЗРОБНИКИ

Гарант ОПП, доцент кафедри захисту інформації, к.т.н., доцент	Олеся ВОЙТОВИЧ
Зав. кафедри захисту інформації, д.т.н., професор	Володимир ЛУЖЕЦЬКИЙ
Доцент кафедри захисту інформації, к.т.н., доцент	Юрій БАРИШЕВ
Доцент кафедри захисту інформації, к.т.н., доцент	Віталій ЛУКІЧОВ

Освітньо-професійну програму розглянуто та схвалено на засіданні Студентської ради факультету інформаційних технологій та комп'ютерної інженерії;

протокол № 10 від 13.01.2023 р.

Голова  Аліна ВОВКОВИНСЬКА

РЕЦЕНЗІЇ-ВІДГУКИ РОБОТОДАВЦІВ

На освітньо-професійну програму надіслали рецензії та відгуки:

Олександр Ульяненков, полковник поліції, начальник Управління протидії кіберзлочинам у Вінницькій обл. Департаменту кіберполіції Національної поліції України

Олександр Томашпольський, директор ТОВ «ВІН ІНТЕРАКТІВ»

Вадим Груша, ТОВ Trustee Global

Людмила Шестопалюк, директор ТОВ «КАСКАД-БЕЗПЕКА»

Олексій Смірнов, д.т.н., проф., завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету

Вступ

Освітньо-професійна програма (далі – ОПП) підготовки магістрів зі спеціальності 125 Кібербезпека та захист інформації розроблена на основі стандарту вищої освіти зі спеціальності 125 Кібербезпека затвердженого наказом МОН України від 18.03.2021 № 332.

1 Профіль освітньо-професійної програми

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Вінницький національний технічний університет, кафедра захисту інформації
Рівень вищої освіти	Другий (магістерський)
Форми здобуття освіти	Денна
Кваліфікація в дипломі	Ступінь вищої освіти – Магістр Спеціальність – 125 Кібербезпека та захист інформації Освітня програма – Безпека інформаційних і комунікаційних систем
Офіційна назва ОП	Безпека інформаційних і комунікаційних систем
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання – 1 рік 4 місяці Мінімум 60% обсягу освітньої програми має бути спрямовано на формування загальних та спеціальних (фахових) компетентностей за спеціальністю, визначених Стандартом вищої освіти. Мінімум 15 кредитів ЄКТС має бути призначено для практики.
Цикл/рівень	7 рівень НРК України, другий цикл FQ-EHEA, 7 рівень EQF-LLL
Передумови	Диплом бакалавра або диплом спеціаліста Програма фахових вступних випробувань для осіб, що здобули попередній рівень вищої освіти за іншими спеціальностями передбачає перевірку набуття особою компетентностей та результатів навчання, що визначені стандартом вищої освіти зі спеціальності 125 Кібербезпека для першого (бакалаврського) рівня вищої освіти.
Мова (и) викладання	Українська, за потреби один або декілька освітніх компонентів можуть викладатися англійською мовою
Акредитація	Сертифікат про акредитацію ОПП УД 02007648 від 08.01.2019 р. термін дії до 01.07.2024 (Протокол АКУ №133 від 27.12.18, Наказ МОНУ від 08.01.2019 №13)
Інтернет-адреса постійного розміщення опису ОП	https://jetiq.vntu.edu.ua/edu_progs/ep_list.php
2 – Мета освітньої програми	
Підготовка висококваліфікованих, конкурентоспроможних фахівців, що володіють загальними та професійними компетентностями необхідними для розв'язання складних задач і проблем у галузі інформаційної та/або кібербезпеки, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог, задля задоволення потреб Вінницького регіону, України та світу; формування творчої	

особистості нового покоління, здатної успішно реалізовувати набуті сучасні професійні компетентності з безпеки інформаційних і комунікаційних систем, інтелектуальний потенціал, навики практичного досвіду та інноваційної діяльності в галузі інформаційних технологій, а також соціально-патріотичні та морально-етичні цінності у глобальному суспільно-економічному просторі[1].	
3 – Характеристика освітньої програми	
Предметна область	**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.
Основний фокус освітньої програми та спеціалізації	Загальна – діяльність з організації та управління в сфері інформаційної та кібербезпеки. Спеціальна – діяльність з організації та управління інформаційною та кібербезпекою шляхом використання технологій проектування систем безпеки інформаційних і комунікаційних систем з урахуванням вимог що висуваються при аудиті кібербезпеки. Ключові слова: кібербезпека, інформаційна безпека, аудит кібербезпеки, інформаційно-комунікаційні системи.
Особливості програми	ОПП спрямована на забезпечення безпеки інформаційних і комунікаційних систем цивільної та критичної інфраструктури, зокрема проектування, розробка, впровадження системи забезпечення інформаційної та / або кібербезпеки, аудит кібербезпеки, з урахуванням потреб регіону та суспільства в цілому.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Професійна діяльність за такими назвами робіт: 2149.2 Професіонал із організації захисту інформації з обмеженим доступом; 2149.2 Професіонал із організації інформаційної безпеки; 2149.2 Фахівець (сфера захисту інформації); 2139.2 Аналітик з безпеки інформаційно-телекомунікаційних систем; 2139.2 Адміністратор мереж і систем. 2310.2 Асистент; Викладач вищого навчального закладу. Права випускників на працевлаштування не обмежуються.
Подальше навчання	Мають право на продовження освіти за третім (освітньо-науковим) рівнем вищої освіти для отримання ступеня доктора філософії. Набуття додаткових кваліфікацій в системі післядипломної освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Лекції, практичні заняття, виконання курсової роботи, лабораторні роботи, самостійна робота на основі навчальних посібників, конспектів лекцій, електронних джерел, консультації із викладачами, семінари, елементи

	дистанційного (онлайн, електронного) навчання, проходження практики на профільних підприємствах чи структурних відділах, в науково-дослідних установах, підготовка кваліфікаційної роботи.
Оцінювання	Методи оцінювання – екзамени, заліки, тести, практика, контрольні, курсові роботи. Формативні (вхідне тестування та поточний контроль): тестування знань або умінь; усні презентації; звіти про лабораторні роботи; аналіз текстів або даних; звіти про практику; огляд джерел тощо. Сумативні (підсумковий контроль): екзамен; залік (за результатами формативного контролю).
6 – Програмні компетентності	
Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності (КЗ)	КЗ1. Здатність застосовувати знання у практичних ситуаціях. КЗ2. Здатність проводити дослідження на відповідному рівні. КЗ3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності). КЗ6. Здатність спілкуватися іноземною мовою у професійній сфері як усно, так і письмово.
Фахові компетентності (КФ)	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. КФ11. Здатність проектувати системи забезпечення кібербезпеки в інформаційних і комунікаційних системах з урахуванням потреб регіону та глобальних світових тенденцій. КФ12. Здатність координувати діяльність із забезпечення безпеки інформаційно-комунікаційних систем.
7 – Програмні результати навчання	
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.
РН24. Проєктувати, розробляти, тестувати системи забезпечення кібербезпеки в інформаційних і комунікаційних системах відповідно до завдань та загроз, що виникають на сучасному етапі розвитку інформаційних технологій.
РН25. Здатність контролювати процес встановлення, впровадження та налаштування компонентів системи щодо захисту інформації.
РН26. Здатність надавати рекомендації щодо планів аварійного відновлення, непередбачених випадків та забезпечення безперервності операцій.

8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Кадрове забезпечення ОПП формується, в основному за рахунок кафедри захисту інформації. До викладання дисциплін залучаються також інші кафедри університету, зокрема кафедра менеджменту та безпеки інформаційних систем. Викладацький склад, який забезпечує реалізацію ОПП, відповідає вимогам, визначеним Ліцензійними умовами провадження освітньої діяльності.
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення відповідає вимогам Ліцензійних умов провадження освітньої діяльності, в тому числі включає в себе спеціалізовані лабораторії (захисту програмного забезпечення, технічного захисту інформації, захисту комп’ютерних мереж), направлені на здобуття спеціальних (фахових) компетентностей, оволодіння практичним навичками забезпечення кібербезпеки, зокрема безпеки інформаційних і комунікаційних систем
Інформаційне та навчально-методичне забезпечення	Включає в себе бібліотечні ресурси, систему підтримки освітнього процесу JetIQ, електронні навчальні ресурси, сайт ВНТУ та сайт кафедри, на яких розміщена основна інформація щодо освітньої діяльності за ОПП.

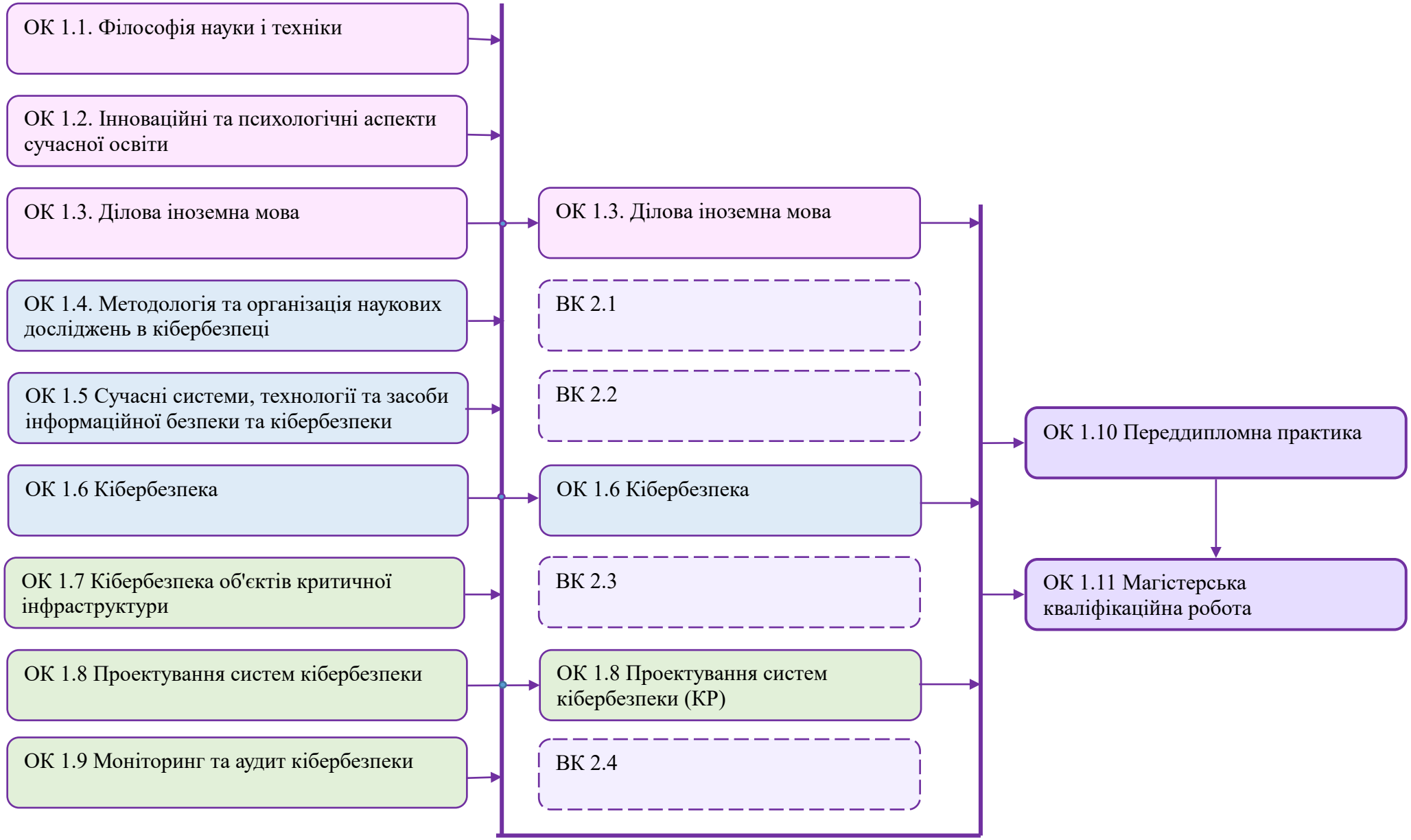
9 – Академічна мобільність Максимальний обсяг кредитів ЄКТС, що може бути перезарахований, становить 25% від загального обсягу освітньої програми (22,5 кредити).	
Національна кредитна мобільність	Здійснюється на підставі укладення угод про співробітництво між ВНТУ та закладами вищої освіти України.
Міжнародна кредитна мобільність	Здійснюється на підставі укладення угод між ВНТУ та групою закладів вищої освіти різних країн за узгодженими та затвердженими у встановленому порядку індивідуальними навчальними планами здобувачів та програмами навчальних дисциплін, а також в рамках міжурядових угод про співробітництво в галузі освіти, міжнародних проектів, в яких ВНТУ приймає участь, грантів та ін.
Навчання іноземних здобувачів вищої освіти	За освітньою програмою передбачено навчання іноземних здобувачів вищої освіти.

2 Перелік компонентів освітньо-професійної програми та їх логічна послідовність

2.1 Перелік компонентів освітньо-професійної програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ (ОК)			
Загальні			
ОК1.1	Філософія науки і техніки	3,0	залік
ОК1.2	Інноваційні та психологічні аспекти сучасної освіти	3,0	залік
ОК1.3	Ділова іноземна мова	3,0	залік
Професійні			
ОК1.4	Методологія та організація наукових досліджень в кібербезпеці	3,0	іспит
ОК1.5	Сучасні системи, технології та засоби інформаційної безпеки та кібербезпеки	3,0	іспит
ОК1.6	Кібербезпека	9,0	іспит
ОК1.7	Кібербезпека об'єктів критичної інфраструктури	4,0	іспит
ОК1.8	Проектування систем кібербезпеки (в т.ч. курсова робота)	5,0	іспит
ОК1.9	Моніторинг та аудит кібербезпеки	4,0	іспит
ОК1.10	Переддипломна практика	15,0	залік
ОК1.11	Магістерська кваліфікаційна робота	15,0	захист
Загальний обсяг обов'язкових компонентів		**67**	
ВИБІРКОВІ КОМПОНЕНТИ ЗА ВІЛЬНИМ ВИБОРОМ СТУДЕНТА (ВК)			
ВК2.1	Освітній компонент 1 з БДВВ	5,0	залік
ВК2.2	Освітній компонент 2 з БДВВ	6,0	залік
ВК2.3	Освітній компонент 3 з БДВВ	6,0	залік
ВК2.4	Освітній компонент 4 з БДВВ	6,0	залік
Загальний обсяг вибіркових компонентів		**23**	
ЗАГАЛЬНИЙ ОБСЯГ ЗА ПЛАНОМ		**90**	

2.2. Структурно-логічна схема освітньо-професійної програми



3 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 ВНТУ (репозитарії) у системі JetIQ. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

4 Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

У ВНТУ функціонує система забезпечення якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості), яка передбачає здійснення таких процедур і заходів:

1) визначення принципів та процедур забезпечення якості вищої освіти;

2) здійснення моніторингу та періодичного перегляду освітніх програм;

3) щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті ВНТУ або в будь-який інший спосіб;

4) забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників;

5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за кожною освітньою програмою;

6) забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;

7) забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації;

8) забезпечення ефективної системи запобігання та виявлення академічного плагіату у наукових працях працівників ВНТУ і здобувачів вищої освіти;

9) інших процедур і заходів.

Система забезпечення якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості) за поданням ВНТУ оцінюється Національним агентством із забезпечення якості вищої освіти або акредитованими ним незалежними установами оцінювання та забезпечення якості вищої освіти на предмет її відповідності вимогам до системи забезпечення якості вищої освіти, що затверджуються Національним агентством із забезпечення якості вищої освіти, та міжнародним стандартам і рекомендаціям щодо забезпечення якості вищої освіти.

5 Перелік нормативних документів, на яких базується освітня програма

– Закон України «Про вищу освіту» - Режим доступу: http://zakon4.rada.gov.ua/laws/show/1556-18 .
– Закон України «Про освіту» - Режим доступу: http://zakon5.rada.gov.ua/laws/show/2145-19.
– Національна рамка кваліфікацій - Режим доступу: https://zakon.rada.gov.ua/laws/show/1341-2011-%D0%BF#Text.
– Постанова Кабінету Міністрів України від 30.12.2015р. .№1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності» - Режим доступу: http://zakon4.rada.gov.ua/laws/show/1187-2015-п/page;
– Стандарт вищої освіти зі спеціальності 125 Кібербезпека затверджений наказом МОН України від 18.03.2021 № 332. - Режим доступу: https://mon.gov.ua/storage/app/media/vyshcha/standarty/2021/03/19/125%20Kiberbezpeka_mahistr_18_03_21_332.docx
– Професійний стандарт 2139.2 Аналітик з безпеки інформаційно-телекомунікаційних систем затверджений Наказом Адміністрації Держспецзвязку 25.11.2022 №715 - Режим доступу: https://register.nqa.gov.ua/uploads/0/435-profesijnij_standart_analitik_z_bezpeki_informacijno_telekomunikacijnih.pdf
– Професійний стандарт 2139.2 Адміністратор мереж і систем затверджений Наказом Адміністрації Держспецзвязку 25.11.2022 №715 - Режим доступу: https://register.nqa.gov.ua/uploads/0/434-profesijnij_standart_administrator_merez_i_sistem.pdf
– Професійний стандарт на групу професій Викладачі закладів вищої освіти затверджений Наказом Міністерства розвитку економіки, торгівлі та сільського господарства України від 23.03.2021 №610. - Режим доступу: https://mon.gov.ua/storage/app/sites/1/pto/standarty/2021/03/25/Standart%20na%20hrupu%20profesiy_Vykladachi%20zakladiv%20vyshchoyi%20osvity_25.03.pdf

Пояснювальна записка

Освітньо-професійна програма містить програмні компетентності, що визначають специфіку підготовки магістрів зі спеціальності 125 Кібербезпека та захист інформації, та програмні результати навчання, які відображають те, що студент повинен знати, розуміти та бути здатним виконувати після успішного завершення освітньої програми. В таблицях 1, 2 (додаток А) наведені матриці відповідності визначених Стандартом зі спеціальності 125 Кібербезпека компетентностей / результатів навчання дескрипторам НРК, а також Матриця відповідності визначених Стандартом результатів навчання та компетентностей. В таблицях 1, 2 (додаток Б) наведені матриці відповідності визначених освітньою програмою результатів навчання (компетентностей) та освітніх компонентів.

Додаток А
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, 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,	Ум1, Ум3	К1	АВ1, АВ2
КЗ2	Зн1,	Ум1, Ум2, Ум3		АВ2, АВ3
КЗ3	Зн1	Ум2, Ум3		АВ1
КЗ4	Зн1	Ум3		АВ1, АВ2
КЗ5	Зн1	Ум2	К1	АВ1
Спеціальні (фахові) компетентності				
КФ1	Зн1	Ум2		АВ2
КФ2	Зн1,	Ум2		АВ2
КФ3	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2
КФ4	Зн1,	Ум1, Ум2	К1	АВ1, АВ2
КФ5	Зн1,	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	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2

Таблиця 2

Матриця відповідності визначених Стандартом результатів навчання та компетентностей

Програмні результати навчання	Компетентності															
	Інтегральна компетентність															
	Загальні компетентності					Спеціальні (фахові) компетентності										
	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11
РН 1	+		+			+										
РН 2		+	+			+	+	+								+
РН 3	+					+										+
РН 4	+	+	+	+		+	+									
РН 5			+		+		+									+
РН 6	+			+		+		+		+	+	+		+		
РН 7	+		+				+									
РН 8	+	+		+	+			+						+	+	
РН 9	+	+	+	+					+					+	+	
РН 10	+		+	+						+				+		
РН 11	+		+	+							+				+	
РН 12	+		+	+					+			+			+	
РН 13	+		+	+									+		+	
РН 14	+		+	+					+					+	+	
РН 15				+	+										+	
РН 16	+	+	+	+				+	+	+	+	+		+	+	+
РН 17								+							+	
РН 18	+			+	+										+	
РН 19	+			+	+	+	+	+	+		+	+	+	+		
РН 20	+	+	+	+	+	+		+								+
РН 21	+	+	+	+		+		+		+		+	+			+
РН 22		+	+	+		+		+								+
РН 23	+		+	+		+	+	+			+	+	+	+		

Додаток Б

Таблиця 1. Матриця забезпечення програмних результатів навчання обов'язковими освітніми компонентами

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11
РН 1			+							+	+
РН 2	+			+	+	+				+	+
РН 3		+		+				+		+	+
РН 4					+	+		+		+	+
РН 5	+			+						+	+
РН 6					+	+			+	+	+
РН 7						+			+	+	+
РН 8					+	+	+	+		+	+
РН 9						+	+		+		
РН 10						+	+	+	+	+	+
РН 11						+	+	+	+	+	
РН 12						+	+		+		
РН 13						+	+			+	+
РН 14						+		+	+		
РН 15	+	+	+	+					+	+	+
РН 16				+		+	+	+	+	+	+
РН 17	+	+		+						+	+
РН 18		+								+	
РН 19				+				+		+	+
РН 20				+		+		+	+	+	+
РН 21				+				+		+	+
РН 22	+			+				+		+	+
РН 23					+	+	+	+	+	+	+
РН 24							+	+	+	+	+
РН 25					+	+	+	+		+	+
РН 26						+	+		+		

Таблиця 2. Матриця відповідності компетентностей обов'язковим освітнім компонентам

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11
КЗ1		+	+	+	+	+	+	+	+	+	+
КЗ2	+			+				+		+	+
КЗ3	+	+		+			+	+	+	+	+
КЗ4				+	+		+	+	+	+	+
КЗ5	+	+	+						+		+
КЗ6			+								+
КФ1					+		+	+		+	+
КФ2						+	+		+	+	+
КФ3					+	+	+	+		+	+
КФ4						+			+	+	+
КФ5				+		+		+	+	+	+
КФ6					+	+			+	+	+
КФ7						+	+		+	+	+
КФ8					+	+	+			+	+
КФ9								+	+	+	+
КФ10		+				+					+
КФ11					+		+	+	+	+	+
КФ12					+	+	+		+		+

ЛИСТОК РЕЄСТРАЦІЇ ЗМІН

Номер зміни	Введення в дію	Що змінилося	Коли вступають в дію
1	Рішення Вченої ради ВНТУ (протокол № 1 від 30.08.23) Наказ №221 від 30.08.23	Зміна мети ОП у відповідності до Стратегії розвитку ВНТУ на 2023-2027 рр. (Протокол Вченої ради ВНТУ № 15 від 29 червня 2023 р.)	з 2023/2024 н.р.