МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖЕНО
Ректор ВНТУ
_____ Віктор БІЛІЧЕНКО
Наказ ВНТУ № 105 від 27.03.2025

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

Кібербезпека інформаційних технологій та систем
Cybersecurity of Information Technologies and Systems

Рівень вищої освіти	другий (магістерський)
Галузь знань	F Інформаційні технології
Спеціальність	F5 Кібербезпека та захист інформації
Освітня кваліфікація	магістр з кібербезпеки та захисту інформації

Розглянуто та схвалено
на засіданні Вченої Ради ВНТУ
Протокол № 10 від 27.03.2025

Вінниця, 2025

ЛИСТ ПОГОДЖЕННЯ

ОПП Кібербезпека інформаційних технологій та систем

Рівень вищої освіти другий (магістерський)

Спеціальність F5 Кібербезпека та захист інформації

Гарант ОПП
к.т.н., доц., завідувач каф. МБІС _____ Василь КАРПІНЕЦЬ

Директор Центру
забезпечення якості освіти
ВНТУ _____ Станіслав ТУЖАНСЬКИЙ

Освітньо-професійну програму розглянуто та схвалено на засіданні кафедри менеджменту та безпеки інформаційних систем;

протокол №13 від «04» 02 2025 р.

Завідувач кафедри МБІС _____ Василь КАРПІНЕЦЬ

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

засіданні Вченої ради факультету менеджменту та інформаційної безпеки;

протокол №8 від «17» 03 2025 р.

Голова _____ Алла КРАЄВСЬКА

засіданні Ради з якості освіти ВНТУ,

протокол №8 від «20» березня 2025 р.

Голова _____ Олександр ПЕТРОВ

ПРЕАМБУЛА

ОПП Кібербезпека інформаційних технологій та систем
Рівень вищої освіти другий (магістерський)
Спеціальність F5 Кібербезпека та захист інформації
Розроблена на основі стандарту вищої освіти (наказ №332 від «18» березня 2021р.)

РОЗРОБНИКИ

Гарант ОПП, завідувач кафедри менеджменту та безпеки інформаційних систем, к. т. н., доцент — Василь КАРПІНЕЦЬ

Голова секції управління інформаційною безпекою кафедри менеджменту та безпеки інформаційних систем, д.т.н., професор — Юрій ЯРЕМЧУК

Доцент кафедри менеджменту та безпеки інформаційних систем, к.т.н., доцент — Анатолій ГРИЦАК

Освітньо-професійну програму розглянуто та схвалено на засіданні Студентської ради факультету менеджменту та інформаційної безпеки;

протокол № 14 від « 26 » лютого 2025 р.

Голова _____ Анастасія РОГОВА

РЕЦЕНЗІЇ ТА ВІДГУКИ РОБОТОДАВЦІВ

На освітньо-професійну програму надіслали рецензії та відгуки:

Рой Віталій Анатолійович, начальник 3-го відділу Управління Держспецзв'язку у Вінницькій області

Прокофьєв Михайло Іванович, доктор технічних наук, заступник директора з наукової роботи ТОВ «Об'єднаний центр захисту інформації», заслужений працівник освіти України

Луканов Максим Всеволодович, фахівець з інформаційної безпеки компанії KNESS Group, випускник спеціальності «Кібербезпека та захист інформації»

Чечелюк Олександр Васильович, старший інженер-програміст ТОВ "Екзіп Текнолоджіз", випускник спеціальності «Кібербезпека»

1 ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

1 – Загальна інформація	
Повна назва ЗВО та структурного підрозділу	Вінницький національний технічний університет, кафедра менеджменту та безпеки інформаційних систем
Рівень вищої освіти	Другий (магістерський)
Освітня кваліфікація	Магістр з кібербезпеки та захисту інформації
Кваліфікація в дипломі	Ступінь вищої освіти – магістр Спеціальність – F5 Кібербезпека та захист інформації Освітня програма – Кібербезпека інформаційних технологій та систем
Офіційна назва освітньої програми	Кібербезпека інформаційних технологій та систем
Форми здобуття освіти	Денна, заочна
Тип диплому та обсяг освітньої програми	Диплом магістра, обсяг освітньої програми 90 кредитів ЄКТС, термін навчання 1 рік і 4 місяці Мінімум 60% обсягу освітньої програми 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	НРК України – 7 рівень, EQF-LLL – 7 рівень, FQ-EHEA – другий цикл
Передумови	Диплом бакалавра або диплом спеціаліста. Програма фахових вступних випробувань для осіб, що здобули попередній рівень вищої освіти за іншими спеціальностями повинна передбачати перевірку набуття особою компетентностей та результатів навчання, що визначені стандартом вищої освіти зі спеціальності 125 для першого (бакалаврського) рівня вищої освіти.
Мова викладання	Українська
Акредитація	Сертифікат про акредитацію освітньої програми №9095 від 03.07.2024. Строк дії 01.07.2029.
Інтернет-адреса постійного розміщення опису освітньої програми	https://jetiq.vntu.edu.ua/edu_progs/ep_list.php?l=2
2 – Мета освітньо-професійної 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 характеризуються 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 кібербезпеки інформаційних технологій та 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.	
3 – Характеристика освітньої програми	
Галузь знань	F Інформаційні технології
Спеціальність	F5 Кібербезпека та захист інформації
Орієнтація освітньої програми	Освітньо-професійна
Предметна область	**Об'єкти вивчення та діяльності:** – 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; – моделі, методи та засоби кібербезпеки інформаційних технологій та систем. **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.
Особливості програми	Формування відповідних компетентностей у сфері інформаційної та кібернетичної безпеки, насамперед, кібербезпеки інформаційних технологій та систем, в умовах нестабільності інформаційного середовища на основі принципів інноваційного розвитку та сучасних інформаційних технологій, поєднуючи ґрунтовну фундаментальну підготовку із сучасною професійною підготовкою, використовуючи при цьому весь науково-технічний потенціал університету в цій сфері, у першу чергу, залучення науково-педагогічного персоналу, апаратури та обладнання відповідних науково-дослідних лабораторій та навчально-наукових центрів, у тому числі тих, що здійснюють свою діяльність відповідно до ліцензії Державної служби спеціального зв’язку та захисту інформації України з надання науково-технічних послуг та

	виконання наукових-дослідних робіт у галузі криптографічного та технічного захисту інформації. Важливим також є орієнтація ОПП на міжнародні професійні програми, включаючи сертифіковані, від провідних компаній-виробників комп'ютерного та мережевого обладнання, програмного забезпечення, технологій та рішень з кібербезпеки, зокрема таких компаній як Microsoft, Cisco, IBM, HCL Technologies, Spyse та ін.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Професіонал здатний виконувати професійну роботу і може займати первинні посади: 2149.2 Професіонал із організації захисту інформації з обмеженим доступом; 2149.2 Професіонал із організації інформаційної безпеки; 2310.2 Асистент. Права випускників на працевлаштування не обмежуються.
Подальше навчання	Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти для здобуття ступеня доктора філософії. Набуття додаткових кваліфікацій в системі післядипломної освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання, самонавчання, проблемно-орієнтоване навчання, лабораторна практика. Лекції, практичні заняття, виконання курсових проектів та робіт, лабораторні роботи, самостійна робота на основі підручників, навчальних посібників, конспектів лекцій, наукових робіт та інших джерел інформації, консультації із викладачами, наукові семінари, технології змішаного навчання, проходження практики на профільних підприємствах, підготовка кваліфікаційної роботи.
Оцінювання	Методи оцінювання – екзамени, тести, практика, контрольні, курсові роботи, есе, презентації. Формативні (вхідне тестування та поточний контроль): тестування знань або умінь; усні презентації; звіти про лабораторні роботи; аналіз текстів або даних; звіти про практику; огляд літератури тощо). Сумативні (підсумковий контроль): екзамен (письмовий з подальшим усним опитуванням); залік (за результатами формативного контролю).

6 – Програмні компетентності	
Інтегральна компетентність	ІК. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності (ЗК)	ЗК 1. Здатність застосовувати знання у практичних ситуаціях. ЗК 2. Здатність проводити дослідження на відповідному рівні. ЗК 3. Здатність до абстрактного мислення, аналізу та синтезу. ЗК 4. Здатність оцінювати та забезпечувати якість виконуваних робіт. ЗК 5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності). ЗК 6. Здатність професійно спілкуватися державною та іноземною мовою як усно, так і письмово.
Фахові компетентності (ФК)	ФК1. 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. ФК 2. 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. ФК 3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. ФК 4. 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. ФК 5. 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. ФК 6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ФК 7. 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. ФК 8. 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. ФК 9. 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. ФК 10. 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. ФК 11. Здатність досліджувати, розробляти та впроваджувати сучасні моделі, методи та засоби забезпечення кібербезпеки інформаційних технологій систем. ФК 12. Здатність формулювати нові гіпотези та наукові задачі у кібербезпеці. Вибирати належні напрями і відповідні методи для розв'язання задач з кібербезпеки інформаційних технологій систем, беручи до уваги наявні ресурси.
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. Досліджувати, розробляти та впроваджувати сучасні моделі, методи та засоби забезпечення кібербезпеки інформаційних технологій систем, аналізувати та проводити оцінювання ефективності та рівня захищеності ресурсів різних класів у ході проведення випробувань згідно встановленої політики безпеки. РН25. Формулювати нові гіпотези та наукові задачі у кібербезпеці, вибирати належні напрями і застосовувати відповідні методи для розв'язання задач з кібербезпеки інформаційних технологій систем, беручи до уваги наявні ресурси. РН26. Використовувати педагогічні технології, які базуються на розумінні психологічних особливостей здобувачів освіти, для викладання та/або наставництва.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Кадрове забезпечення ОПП формується, в основному за рахунок кафедри менеджменту та безпеки інформаційних систем. До викладання дисциплін залучаються також провідні викладачі інших кафедр університету. 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 сучасні лабораторії Центру інформаційних технологій та захисту інформації, зокрема комп'ютерні класи мережевої академії Cisco та IT Академії Microsoft, Науково-дослідну лабораторію технічного захисту інформації.
Інформаційне та навчально-методичне забезпечення	Включає в себе ресурси науково-технічної бібліотеки, систему підтримки освітнього процесу JetIQ, електронні навчальні ресурси, сайт ВНТУ та сайт кафедри, на яких розміщена основна інформація щодо освітньої діяльності за ОПП.

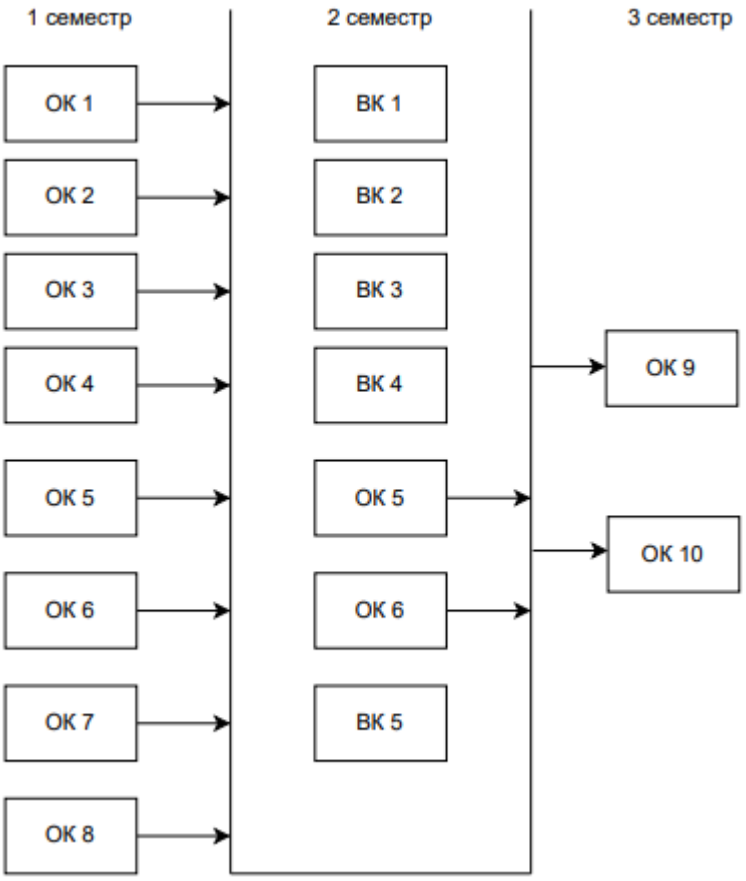
9 – Академічна мобільність	
Максимальний обсяг кредитів ЄКТС, що може бути перезарахований, становить 25% від загального обсягу освітньої програми.	
Національна кредитна мобільність	Здійснюється на підставі укладення угод про співробітництво між ВНТУ та закладами вищої освіти України.
Міжнародна кредитна 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 бере участь, грантів та ін.
Навчання іноземних здобувачів вищої освіти	За даною 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 ОК	Компоненти ОПП	Кількість кредитів	Форма підсумкового контролю
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ			
Загальні			
ОК 1	Ділова іноземна мова	3,0	залік
ОК 2	Інноваційні та психологічні аспекти сучасної освіти	3,0	залік
Професійні			
ОК 3	Методологія та організація наукових досліджень у кібербезпеці	3,0	іспит
ОК 4	Сучасні системи, технології та засоби інформаційної безпеки та кібербезпеки	3,0	іспит
ОК 5	Кібербезпека	10,0	іспит
ОК 6	Системний аналіз і технології підтримки прийняття рішень (в т. ч. курсова робота)	6,0	іспит
ОК 7	Кібербезпека інформаційних технологій та систем	4,0	залік
ОК 8	Аудит інформаційної безпеки	5,0	іспит
ОК 9	Переддипломна практика	15,0	залік
ОК 10	Магістерська кваліфікаційна робота	15,0	
Загальний обсяг обов'язкових компонентів		**67**	
ВИБІРКОВІ КОМПОНЕНТИ			
ВК 1	Освітній компонент 1 з БЗДВВ	3,0	залік
ВК 2	Освітній компонент 2 з БПДВВ	5,0	залік
ВК 3	Освітній компонент 3 з БПДВВ	5,0	залік
ВК 4	Освітній компонент 4 з БПДВВ	5,0	залік
ВК 5	Освітній компонент 5 з БПДВВ	5,0	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 магістерської 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.

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 ВНТУ та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті ВНТУ та 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 здобувачів вищої освіти, 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, які забезпечують належний рівень якості вищої освіти.

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» 01.07.2014 №1556-VII - [Режим доступу: http://zakon4.rada.gov.ua/laws/show/1556-18];

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Режим доступу: https://zakon2.rada.gov.ua/laws/show/80/94-вр];

– Закон України «Про основні засади забезпечення кібербезпеки України» - відомості Верховної Ради (ВВР), 2017, №45, ст.403;

– 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];

– Постанова Кабінету Міністрів України «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 29.04.2015 р. №266. [Режим доступу: http://zakon.rada.gov.ua/laws/show/266-2015-п];

– Національний класифікатор України: "Класифікатор професій» ДК 003:2010;

– Наказ МОН України №1074 «Про затвердження стандарту вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для першого (бакалаврського) рівня вищої освіти» від 04.10.2018 р.;

–«Доктрина інформаційної безпеки України», затверджено Указом Президента України від 25 лютого 2017 року №47/2017. [Режим доступу: https://www.president.gov.ua/documents/472017-21374];

– Рішення Ради національної безпеки і оборони України «Про стратегію кібербезпеки України» від 14 травня 2021 року [Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#Text];

– Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27 вересня 1999 р. №1229;

– Положення про порядок здійснення криптографічного захисту інформації в України, затверджене Указом Президента України від 22 травня 1998 р. №505;

– Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29 березня 2006 р. №373.

Пояснювальна записка

Освітньо-професійна програма містить програмні компетентності, що визначають специфіку підготовки магістрів зі спеціальності F5 «Кібербезпека та захист інформації» та програмні результати навчання, які виражають те, що здобувач повинен знати, розуміти та бути здатним виконувати після успішного завершення освітньої програми. В таблицях 1, 2 наведені матриці відповідності визначених освітньою програмою результатів навчання дескрипторам НРК та компетентностям, а у таблицях 3, 4 наведені матриці відповідності програмних результатів навчання та компетентностей обов'язковим освітнім компонентам.

Таблиця 1

Матриця відповідності 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				
ЗК1	Зн1,	Ум1, Ум3	К1	АВ1, АВ2
ЗК2	Зн1,	Ум1, Ум2, Ум3		АВ2, АВ3
ЗК3	Зн1	Ум2, Ум3		АВ1
ЗК4	Зн1	Ум3		АВ1, АВ2
ЗК5	Зн1	Ум2	К1	АВ1
ЗК6	Зн1	Ум2	К1	АВ2
Спеціальні (фахові) компетентності				
ФК1	Зн1	Ум2		АВ2
ФК2	Зн1,	Ум2		АВ2
ФК3	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2
ФК4	Зн1,	Ум1, Ум2	К1	АВ1, АВ2
ФК5	Зн1,	Ум1, Ум2	К1	АВ1, АВ2
ФК6	Зн1	Ум1, Ум2	К1	АВ1
ФК7	Зн1	Ум1, Ум2	К1	АВ1
ФК8	Зн1	Ум1, Ум2	К1	АВ1
ФК9	Зн1	Ум1, Ум2	К1	АВ1
ФК10	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2
ФК11	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2
ФК12	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2

Таблиця 2

Матриця відповідності
результатів навчання та компетентностей

Програмні результати навчання	Компетентності																	
	Інтегральна компетентність																	
	Загальні компетентності						Спеціальні (фахові) компетентності											
	ЗК 1	ЗК 2	ЗК 3	ЗК 4	ЗК 5	ЗК 6	ФК 1	ФК 2	ФК 3	ФК 4	ФК 5	ФК 6	ФК 7	ФК 8	ФК 9	ФК 10	ФК 11	ФК 12
РН 1	+		+			+	+											
РН 2		+	+				+	+	+								+	+
РН 3	+						+											+
РН 4	+	+	+	+			+	+										
РН 5			+		+			+									+	+
РН 6	+			+			+		+		+	+	+		+			
РН 7	+		+					+										
РН 8	+	+		+	+				+						+	+		
РН 9	+	+	+	+						+					+	+		
РН 10	+		+	+							+				+			
РН 11	+		+	+								+				+		
РН 12	+		+	+						+			+			+		+
РН 13	+		+	+										+		+		
РН 14	+		+	+						+					+	+		
РН 15				+	+											+	+	+
РН 16	+	+	+	+					+	+	+	+	+		+	+	+	
РН 17									+							+		+
РН 18	+			+	+											+		
РН 19	+			+	+		+	+	+	+		+	+	+	+			
РН 20	+	+	+	+	+		+		+								+	+
РН 21	+	+	+	+			+		+		+		+	+				
РН 22		+	+	+			+		+									+
РН 23	+		+	+			+	+	+			+	+	+	+			
РН 24			+														+	
РН 25			+										+	+				+
РН 26																		

Таблиця 3

Матриця відповідності
програмних результатів навчання обов'язковим освітнім компонентам

Програмні результати навчання	**Обов'язкові освітні компоненти**									
	ОК 1	ОК2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10
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 4

Матриця відповідності
компетентностей обов'язковим освітнім компонентам

Компетентності	**Обов'язкові освітні компоненти**									
	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10
ІК	+	+	+	+	+	+	+	+	+	+
ЗК1		+	+	+	+	+	+	+	+	+
ЗК2	+		+	+				+	+	+
ЗК3		+	+	+		+		+	+	+
ЗК4			+	+			+		+	+
ЗК5	+	+						+	+	
ЗК6	+					+		+	+	+
ФК1				+			+		+	+
ФК2					+		+	+	+	+
ФК3			+	+	+		+		+	+
ФК4					+		+	+	+	+
ФК5			+	+	+	+	+		+	+
ФК6					+	+	+		+	+
ФК7					+		+		+	+
ФК8			+	+	+		+		+	+
ФК9							+	+	+	+
ФК10			+		+		+	+	+	+
ФК11				+	+		+		+	+
ФК12			+		+	+	+			+

ЛИСТОК РЕЄСТРАЦІЇ ЗМІН

Номер зміни	Введення в дію	Що змінилося	Коли вступають в дію