

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖЕНО

Ректор ВНТУ

Віктор БІЛЧЕНКО

Наказ ВНТУ № 20 від 26.01.2023р.



ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

**Управління інформаційною безпекою**

**Information Security Management**

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

Розглянуто та схвалено

на засіданні Вченої Ради ВНТУ

Протокол № 6 від 26.01.2023р.

Вінниця, 2023

## ЛИСТ ПОГОДЖЕННЯ

### ОПП Управління інформаційною безпекою

Рівень вищої освіти    другий (магістерський)


Спеціальність            125 Кібербезпека та захист інформації

Гарант ОПП  
к.т.н., доц. каф. ВМ



Наталія САЧАНЮК-  
КАВЕЦЬКА

Директор Центру  
забезпечення якості освіти  
ВНТУ



Олеся ВОЙТОВИЧ

Освітньо-професійну програму розглянуто та схвалено на засіданні кафедри менеджменту та безпеки інформаційних систем;  
протокол № 8 від 17 грудня 2022 р.

Завідувач кафедри МБІС



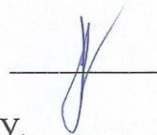
Василь КАРПІНЕЦЬ

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

засіданні Вченої ради факультету менеджменту та інформаційної безпеки;

протокол № 5 від 18 січня 2023 р.

Голова



Ірина ЄПІФАНОВА

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

Голова



Олександр ПЕТРОВ

## ПРЕАМБУЛА

### ОПП Управління інформаційною безпекою

Рівень вищої освіти           другий (магістерський)  
Спеціальність                 125 Кібербезпека та захист інформації  
Розроблена на основі стандарту вищої освіти (наказ № 332 від «18» березня 2021 р.)

### РОЗРОБНИКИ

Гарант ОПП, к.т.н., доц. каф. ВМ	Наталія САЧАНЮК-КАВЕЦЬКА
Голова секції УБ каф. МБІС, д.т.н., професор	Юрій ЯРЕМЧУК
Завідувач кафедри МБІС, к.т.н., доцент	Василь КАРПІНЕЦЬ

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

протокол № 1 від 05 січня 2023 р.

Голова



Мирослава ГРНИК

### РЕЦЕНЗІЇ-ВІДГУКИ РОБОТОДАВЦІВ

На освітньо-професійну програму надіслали рецензії та відгуки:

Грималовський Микола Миколайович, начальник 3-го відділу Управління Державної служби спеціального зв'язку та захисту інформації у Вінницькій області

Прокоф'єв Михайло Іванович, доктор технічних наук, директор Науково-дослідного центру систем технічного захисту інформації "ТЕЗІС" НТУУ «КПІ ім. Ігоря Сікорського», віце-президент Асоціації захисників інформації "АЗІС", Заслужений працівник освіти України

Волинець Олександр Юрійович, керівник проектів в ІТ компанії Morebis, випускник кафедри менеджменту та безпеки інформаційних систем ВНТУ за спеціальністю "Управління інформаційною безпекою"

Безпалый Кирило Валерійович, старший інженер розробник в ІТ компанії Exadel, випускник кафедри менеджменту та безпеки інформаційних систем ВНТУ за спеціальністю "Управління інформаційною безпекою"

## Вступ

Освітньо-професійна програма (ОПП) «Управління інформаційною безпекою» є нормативним документом, у якому визначається нормативний термін та зміст навчання, нормативні форми державної атестації, встановлюються вимоги до змісту, обсягу, рівня освіти та професійної підготовки фахівця освітньо-кваліфікаційного рівня магістра за спеціальністю 125 «Кібербезпека та захист інформації».

### 1 Профіль освітньо-професійної програми

<b>1 – Загальна інформація</b>	
<b>Повна назва вищого навчального закладу та структурного підрозділу</b>	Вінницький національний технічний університет, кафедра менеджменту та безпеки інформаційних систем
<b>Рівень вищої освіти</b>	Другий рівень
<b>Ступінь, що присвоюється</b>	Магістр
<b>Назва галузі</b>	12 «Інформаційні технології»
<b>Назва спеціальності</b>	125 «Кібербезпека та захист інформації»
<b>Офіційна назва освітньої програми</b>	Управління інформаційною безпекою
<b>Форми здобуття освіти</b>	Денна, заочна, дистанційна, дуальна
<b>Освітня кваліфікація</b>	Магістр з кібербезпеки
<b>Кваліфікація в дипломі</b>	Ступінь вищої освіти – Магістр Спеціальність – 125 Кібербезпека та захист інформації
<b>Опис предметної області</b>	<b>Об'єкти вивчення:</b> – 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.

### **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.

<b>Тип диплому та обсяг освітньої програми</b>	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.
<b>Цикл/рівень</b>	7 рівень НРК України, другий цикл FQ-ЕНЕА, 7 рівень EQF-LLL
<b>Передумови</b>	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.
<b>Мова (и) викладання</b>	Українська
<b>Акредитація</b>	Сертифікат про акредитацію освітньої програми УД 02007647 терміном дії до 01.07.2024 р.
<b>Інтернет-адреса постійного розміщення опису освітньої програми</b>	<a href="https://vntu.edu.ua/uk/information-for-enrollee/progmagbak.html">https://vntu.edu.ua/uk/information-for-enrollee/progmagbak.html</a>
<b>2 – Мета освітньої програми</b>	
Формування творчої особистості нового покоління, здатної успішно реалізовувати набуті сучасні професійні компетентності з управління інформаційної безпеки, інтелектуальний потенціал, навички практичного досвіду та інноваційної діяльності в галузі кібербезпеки та захисту інформації, а також соціально-патріотичні та морально-етичні цінності у глобальному суспільно-економічному просторі <sup>1</sup> .	
<b>3 – Характеристика освітньої програми</b>	
<b>Предметна область (галузь знань, спеціальність, спеціалізація)</b>	Галузь знань – 12 «Інформаційні технології» Спеціальність – 125 «Кібербезпека та захист інформації»

<b>Орієнтація освітньої програми</b>	Освітньо-професійна програма орієнтована на принципи супроводу систем та комплексів інформаційної та кібернетичної безпеки; сучасні моделі та методи захисту інформаційно-комунікаційних технологій та відповідного програмно-апаратного забезпечення; теорії, моделі та принципи управління інформаційною та кібернетичною безпекою, а також доступом до інформаційних ресурсів.
<b>Основний фокус освітньої програми та спеціалізації</b>	Загальна вища освіта у галузі знань інформаційних технологій, інформаційної та кібернетичної безпеки, з поглибленою спеціальною підготовкою у сфері управління інформаційною (кібер-) безпекою. Програма спрямована на підготовку професіоналів, здатних застосувати математичні основи, алгоритмічні принципи в моделюванні, проектуванні, розробці, впровадженні та супроводі інформаційних технологій та систем задля забезпечення та управління інформаційною та кібернетичною безпекою.
<b>Особливості програми</b>	Формування відповідних компетентностей у сфері інформаційної та кібернетичної безпеки, а також управління інформаційною (кібер-) безпекою 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.
<b>4 – Придатність випускників до працевлаштування та подальшого навчання</b>	
<b>Придатність до працевлаштування</b>	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.
<b>Подальше навчання</b>	Можливість продовження освіти за третім (освітньо-науковим) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.
<b>5 – Викладання та оцінювання</b>	
<b>Викладання та навчання</b>	Лекції, практичні заняття, виконання курсових робіт, дослідницькі лабораторні роботи, самостійна робота на основі підручників, навчальних посібників та конспектів лекцій, консультації із викладачами, наукові семінари, демонстраційні класи, елементи дистанційного (онлайн, електронного) навчання проходження практики на підприємствах та в науково-дослідних установах, підготовка кваліфікаційної роботи.
<b>Оцінювання</b>	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).
<b>6 – Програмні компетентності</b>	
<b>Інтегральна компетентність</b>	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
<b>Загальні компетентності (ЗК)</b>	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

	<p>експертами з інших галузей знань / видів економічної діяльності).</p> <p>ЗК 6. Здатність професійно спілкуватися державною та іноземною мовою як усно, так і письмово.</p>
<p><b>Фахові компетентності (ФК)</b></p>	<p>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.</p> <p>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.</p> <p>ФК 3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.</p> <p>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.</p> <p>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.</p> <p>ФК 6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.</p> <p>ФК 7. Здатність досліджувати, розробляти та</p>

	<p>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>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.</p> <p>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.</p> <p>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.</p> <p>ФК 11. Здатність аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем з управління інформаційною безпекою, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.</p> <p>ФК 12. Здатність формулювати нові гіпотези та наукові задачі у кібербезпеці. Вибирати належні напрями і відповідні методи для розв'язання задач з управління інформаційною безпекою, беручи до уваги наявні ресурси.</p>
<b>7 – Програмні результати навчання</b>	
	<p>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</p>

безпеки та/або кібербезпеки.

PH2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

PH3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

PH4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

PH5. 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.

PH6. 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 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 натурального, 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. Аналізувати, інтегрувати та приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем з управління інформаційною безпекою, які характеризуються комплексністю та неповною визначеністю умов.

РН25. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

## **8 – Ресурсне забезпечення реалізації програми**

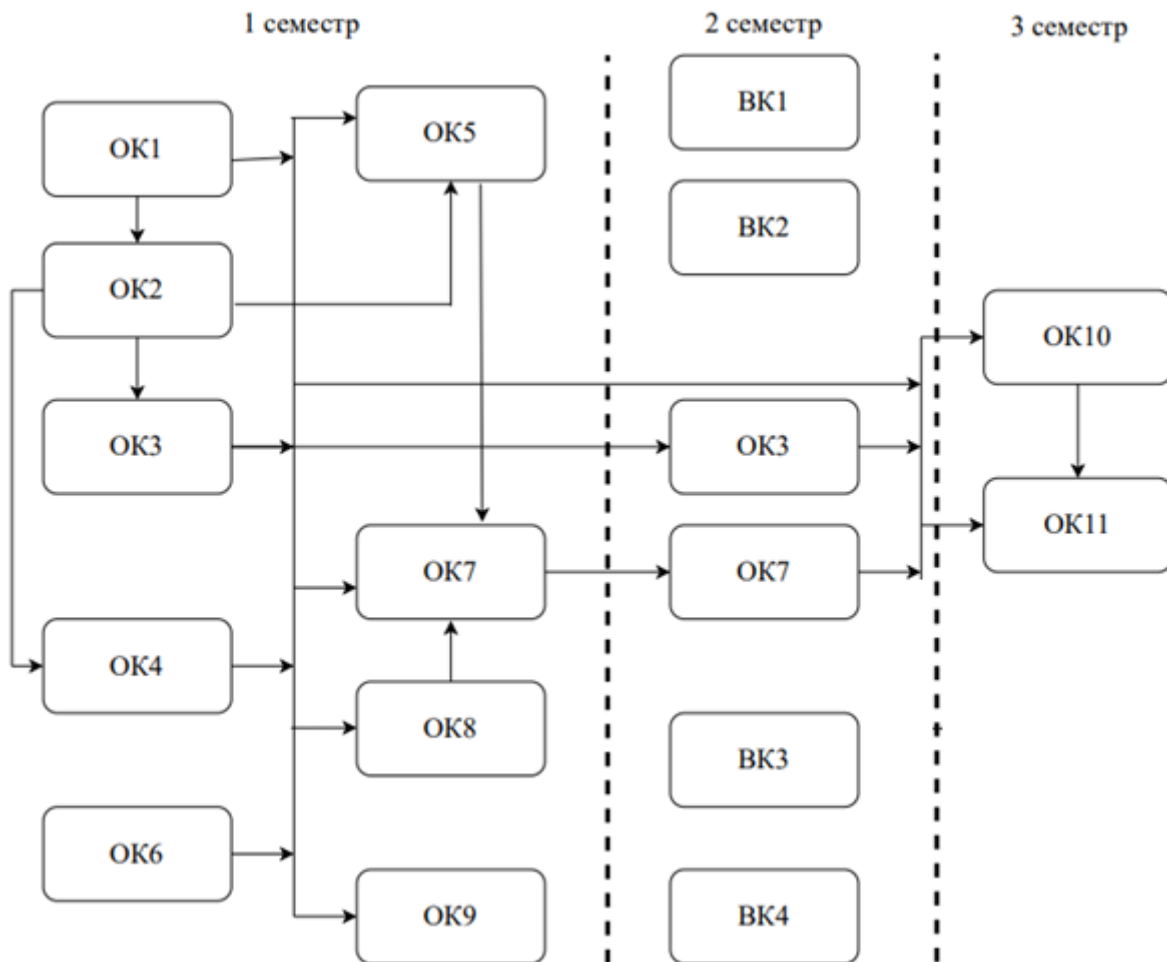
<b>Кадрове забезпечення</b>	Кадрове забезпечення ОПП формується, в основному за рахунок кафедри менеджменту та безпеки інформаційних систем. До викладання дисциплін залучаються також інші кафедри факультету менеджменту та інформаційної безпеки, і університету. Кадрове забезпечення ОПП відповідає вимогам, визначеним Ліцензійними умовами провадження освітньої діяльності.
<b>Матеріально-технічне забезпечення</b>	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 ІТ Академії Microsoft, Науково-дослідну лабораторію технічного захисту інформації.
<b>Інформаційне та навчально-методичне забезпечення</b>	Відповідно до вимог Ліцензійних умов провадження освітньої діяльності 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 ОП.
<b>9 – Академічна мобільність</b>	
<b>Національна кредитна мобільність</b>	Здійснюється на підставі укладення угод про співробітництво між Університетом та закладами вищої освіти України.
<b>Міжнародна кредитна мобільність</b>	Здійснюється на підставі укладення угод між Університетом та групою закладів вищої освіти різних країн за узгодженими та затвердженими у встановленому порядку індивідуальними навчальними планами студентів та програмами навчальних дисциплін, а також в рамках міжурядових угод про співробітництво в галузі освіти, міжнародних проектів, в яких Університет приймає участь, грантів та ін.
<b>Навчання іноземних здобувачів вищої освіти</b>	За даною освітньою програмою передбачено навчання іноземних здобувачів вищої освіти

## 2 Перелік компонент освітньо-професійної програми та їх логічна послідовність

### 2.1 Перелік компонент освітньо-професійної програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
<b>ОБОВ'ЯЗКОВІ КОМПОНЕНТИ</b>			
Загальні			
1.1.	Філософія науки і техніки	3,0	залік
1.2.	Інноваційні та психологічні аспекти сучасної освіти	3,0	залік
1.3.	Ділова іноземна мова	3,0	залік
Професійні			
1.4.	Системний аналіз і технології підтримки прийняття рішень (в т. ч. курсова робота)	5,0	іспит
1.5.	Методологія та організація наукових досліджень у кібербезпеці	3,0	іспит
1.6.	Сучасні системи, технології та засоби інформаційної безпеки та кібербезпеки	3,0	іспит
1.7.	Кібербезпека	9,0	іспит
1.8.	Управління інформаційною безпекою	4,0	залік
1.9.	Аудит інформаційної безпеки	4,0	іспит
1.10.	Переддипломна практика	15,0	залік
1.11.	Магістерська кваліфікаційна робота	15,0	
<b>Загальний обсяг обов'язкових компонент</b>		<b>67</b>	
<b>ВИБІРКОВІ КОМПОНЕНТИ ЗА ВІЛЬНИМ ВИБОРОМ СТУДЕНТА</b>			
2.1.	Освітній компонент 1 з БДВВ	5,0	залік
2.2.	Освітній компонент 2 з БДВВ	6,0	залік
2.3.	Освітній компонент 3 з БДВВ	6,0	залік
2.4.	Освітній компонент 4 з БДВВ	6,0	залік
		<b>23</b>	
<b>ЗАГАЛЬНИЙ ОБСЯГ ЗА ПЛАНОМ</b>		<b>90</b>	

## 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.

### 4 Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

У Вінницькому національному технічному університеті 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 вищого навчального закладу та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті вищого навчального закладу, на інформаційних стендах 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 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 вищих навчальних закладів і здобувачів вищої освіти;

9) інших процедур і заходів, які забезпечують належний рівень 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: <http://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 [Режим доступу: <http://www.003.com>];
- 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 27.01.2016 р., уведеного в дію Указом Президента України від 15.03.2016 р. №96. [Режим доступу: <https://www.president.gov.ua/documents/2422016-20141>];
- 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 Україні, 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 125 «Кібербезпека та захист інформації» та програмні результати навчання, які виражають те, що студент 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

<b>Класифікація компетентностей (результатів навчання) за НРК</b>	<b>Знання Зн1</b> 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	<b>Уміння/Навички Ум1</b> Спеціалізовані уміння/навички розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур <b>Ум2</b> Здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах <b>Ум3</b> Здатність розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності	<b>Комунікація К1</b> Зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і нефахівців, зокрема до осіб, які навчаються	<b>Відповідальність і автономія АВ1</b> Управління робочими або навчальними процесами, які є складними, непередбачуваними та потребують нових стратегічних підходів <b>АВ2</b> Відповідальність за внесок до професійних знань і практики та/або оцінювання результатів діяльності команд та колективів <b>АВ3</b> Здатність продовжувати навчання з високим ступенем автономії
<b>Загальні компетентності</b>				
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
<b>Спеціальні (фахові) компетентності</b>				
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

**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
PH 1	+		+			+	+											
PH 2		+	+				+	+	+								+	+
PH 3	+						+											+
PH 4	+	+	+	+			+	+										
PH 5			+		+			+									+	+
PH 6	+			+			+		+		+	+	+		+			
PH 7	+		+					+										
PH 8	+	+		+	+				+						+	+		
PH 9	+	+	+	+						+					+	+		
PH 10	+		+	+							+				+			
PH 11	+		+	+								+				+		
PH 12	+		+	+						+			+			+		+
PH 13	+		+	+										+		+		
PH 14	+		+	+						+					+	+		
PH 15				+	+											+	+	+
PH 16	+	+	+	+					+	+	+	+	+		+	+	+	
PH 17									+							+		+
PH 18	+			+	+											+		
PH 19	+			+	+		+	+	+	+		+	+	+	+			
PH 20	+	+	+	+	+		+		+								+	+
PH 21	+	+	+	+			+		+		+		+	+				
PH 22		+	+	+			+		+									+
PH 23	+		+	+			+	+	+			+	+	+	+			
PH 24			+														+	
PH 25			+											+				+

**Матриця відповідності  
програмних результатів навчання обов'язковим освітнім компонентам**

Програмні результати навчання	Обов'язкові освітні компоненти										
	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11
PH 1			+								
PH 2	+			+	+	+	+		+	+	+
PH 3		+		+	+					+	+
PH 4						+					+
PH 5	+			+	+	+	+		+		+
PH 6						+			+	+	+
PH 7							+		+	+	+
PH 8						+				+	+
PH 9				+			+	+		+	+
PH 10									+	+	+
PH 11							+	+		+	
PH 12							+			+	+
PH 13							+			+	+
PH 14						+			+	+	
PH 15	+	+								+	+
PH 16				+				+		+	
PH 17	+	+								+	
PH 18		+					+	+			
PH 19					+		+			+	+
PH 20					+		+				+
PH 21							+			+	+
PH 22					+					+	+
PH 23						+					
PH 24				+				+		+	+
PH 25								+		+	+

**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	ОК 11
ЗК1			+	+	+	+	+	+	+	+	+
ЗК2	+				+						+
ЗК3	+	+		+	+			+	+	+	+
ЗК4				+				+		+	
ЗК5	+	+	+							+	
ЗК 6			+							+	+
ФК1						+				+	+
ФК2							+		+	+	+
ФК3						+	+			+	+
ФК4							+	+		+	
ФК5				+	+					+	+
ФК6						+	+	+		+	
ФК7							+	+	+	+	+
ФК8							+			+	+
ФК9									+	+	
ФК10		+		+						+	
ФК11				+				+		+	+
ФК12	+							+			+

