

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ



ЗАТВЕРДЖЕНО

Ректор ВНТУ

_____ В.В. Грабко

Наказ ВНТУ № 139 від «24» 06 2020р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

Управління інформаційною безпекою

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

Розглянуто та схвалено
на засіданні Вченої Ради
ВНТУ Протокол № 12 від
«24» 06 2020р.

Вінниця, 2020

ЛИСТ ПОГОДЖЕННЯ

ОПП Управління інформаційною безпекою

Рівень вищої освіти другий (магістерський)

Спеціальність 125 Кібербезпека

Гарант ОПП
к.т.н., проф. каф. МБІС



А.О. Азарова

Директор Центру
забезпечення якості освіти
ВНТУ



О. П. Войтович

Освітньо-професійну програму розглянуто та схвалено на засіданні кафедри менеджменту та безпеки інформаційних систем;
протокол № 14 від « 31 » 03 2020р.

Зав. кафедри МБІС



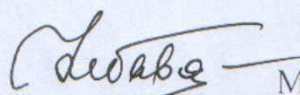
В. В. Карпинець

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

засіданні Вченої ради факультету менеджменту та інформаційної безпеки;

протокол № 7 від « 18 » 05 2020 р.

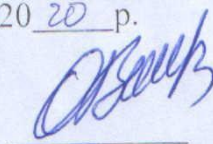
Голова



М. І. Небава

засіданні Методичної ради ВНТУ,
протокол № 12 від « 18 » 06 2020 р.

Голова



О. М. Васілевський

ПРЕАМБУЛА

ОПП Управління інформаційною безпекою
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека

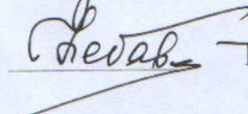
РОЗРОБНИКИ

Гарант ОПП, к.т.н., проф. каф. МБІС



А. О. Азарова

Декан факультету менеджменту та
інформаційної безпеки, к.т.н., професор



М. І. Небава

Завідувач кафедри МБІС, к.т.н., доцент

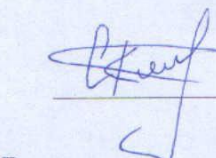


В. В. Карпінєць

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

протокол № 10 від «9» 06 2020 р.

Голова



К. Р. Салієва

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

Овчарук Сергій Володимирович, заступник начальника Відділу протидії кіберзлочинам у Вінницькій області

Карпінський Микола Петрович, доктор технічних наук, професор, завідувач кафедри комп'ютерних наук та автоматички, Уповноважений ректора у справах Східної Європи Університету у Бельсько-Бялій

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 проєктів 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"

Зміст

Вступ.....	5
1. Профіль освітньо-професійної програми.....	5
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність.....	14
3. Форми атестації здобувачів вищої освіти.....	16
4. Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти.....	16
5. Перелік нормативних документів, на яких базується освітня програма.....	17
Пояснювальна записка.....	18
Додаток А. Матриці відповідності.....	19

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».

1 Профіль освітньо-професійної програми

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Вінницький національний технічний університет, кафедра менеджменту та безпеки інформаційних систем
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр Магістр з кібербезпеки
Офіційна назва освітньої програми	Управління інформаційною безпекою
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання – 1 рік 4 місяці
Цикл/рівень	8 рівень НРК України, другий цикл FQ-EHEA, 7 рівень EQF-LLL
Передумови	Наявність ступеня бакалавра
Мова (и) викладання	Українська
Термін дії освітньої програми	5 років
Інтернет-адреса постійного розміщення опису освітньої програми	http://mbis.vntu.net/wp-content/uploads/2020/07/Осв_програма_УБ_mag.pdf
2 – Мета освітньої програми	
Підготовка фахівців в галузі інформаційних технологій зі спеціальності 125 «Кібербезпека» з управління інформаційною та/або кібербезпекою, здатних до практичної реалізації отриманих знань в науці, виробництві та бізнесі. Розвиток творчого наукового потенціалу молоді, намагання до самоосвіти та саморозвитку особистості як життєвої необхідності.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація)	Галузь знань – 12 «Інформаційні технології» Спеціальність – 125 «Кібербезпека»

Орієнтація освітньої програми	Освітньо-професійна програма орієнтована на принципи супроводу систем та комплексів кібербезпеки; теорії, моделі та принципи управління доступом до інформаційних ресурсів; необхідного рівня захищеності інформації; сучасні інформаційно-комунікаційні технології; сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Методи, методики та технології	Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення кібербезпеки інформаційних систем.
Інструменти та обладнання	Системи розробки, забезпечення, моніторингу та контролю процесів інформаційної безпеки; сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Основний фокус освітньої програми та спеціалізації	Загальна: акцент на системному аналізі здобутків вітчизняних та зарубіжних дослідників для прийняття обґрунтованих професійних рішень щодо забезпечення безпеки інформації, управління інформаційною та/або кібербезпекою за умов невизначеності та мінливості зовнішнього середовища з врахуванням резервів та можливостей інноваційного розвитку внутрішнього середовища підприємства на основі широкого використання сучасних інформаційних технологій.
Особливості програми	Формування відповідних компетентностей в умовах нестабільності інформаційного середовища на основі принципів інноваційного розвитку та сучасних інформаційних технологій.
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	Можливість навчання за програмою третього (освітньо-наукового) рівня вищої освіти.

5 – Викладання та оцінювання

Викладання та навчання	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.
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	Здатність особи розв'язувати складні задачі і проблеми у галузі інформаційної безпеки та/або кібербезпеки, а також у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.
Загальні компетентності (ЗК)	ЗК 1. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК 2. Здатність проведення досліджень на відповідному рівні. ЗК 3. Здатність професійно спілкуватися державною мовою як усно, так і письмово. ЗК 4. Здатність професійно спілкуватися іноземною мовою як усно, так і письмово. ЗК 5. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК 6. Здатність до абстрактного мислення, аналізу та синтезу. ЗК 7. Здатність оцінювати та забезпечувати якість виконуваних робіт. ЗК 8. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

**Спеціальні (фахові)
компетентності (СК)**

СК 1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, науково-технічні розробки, фізичні та математичні фундаментальні знання і моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у галузі інформаційної безпеки та/або кібербезпеки.

СК 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 з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

СК 3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

СК 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.

СК 5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення уразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

СК 6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

СК 7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також

	<p>надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.</p> <p>СК 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>СК 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>СК 10. Здатність проводити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також здійснювати наукові дослідження в сфері безпеки інформаційних систем і технологій, відповідно вітчизняним та світовим стандартам і вимогам.</p>
--	---

7 – Програмні результати навчання

	<p>РН 1. Розв'язувати складні науково-технічні та прикладні завдання та проблеми з інформаційної безпеки та/або кібербезпеки, що потребують оновлення та інтеграції фундаментальних знань, у тому числі в умовах неповної інформації та суперечливих вимог.</p> <p>РН 2. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також здійснювати наукові дослідження в сфері технічного та криптографічного захисту інформації у кіберпросторі.</p> <p>РН 3. Вільно користуватися 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.</p> <p>РН 4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні</p>
--	--

інформаційні технології, науково-технічні методи і моделі, фізичні та математичні фундаментальні знання в галузі інформаційної безпеки та/або кібербезпеки.

РН 5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міжпредметному рівні, зокрема з використанням інженерно-технічних і математичних наук, а також напрямів технологій створення та використання спеціалізованого програмного забезпечення.

РН 6. Критично оцінювати захищеність систем, комплексів та засобів кіберзахисту, технологій створення та використання спеціалізованого програмного забезпечення, зокрема з використанням сучасних програмних та програмно-апаратних рішень та сучасних підходів.

РН 7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН 8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

РН 9. Проводити аналіз, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі концептуальних питань стратегії і політики інформаційної безпеки.

РН 10. Досліджувати та проводити системний аналіз забезпечення безперервності бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, проводити аналіз ризиків та визначати оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН 11. Аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН 12. Проводити дослідження, 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.

РН 13. Проводити дослідження, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також проводити аналіз і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

РН 14. Здійснювати аналіз, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів в галузі інформаційної та\або кібербезпеки в цілому.

РН 15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та\або кібербезпеки, а також знання та пояснення, що їх обґрунтовують.

РН 16. 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.

РН 17. 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.

РН 18. Проводити науково-педагогічну діяльність, планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та\або кібербезпеки.

РН 19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розуміти основні аспекти впровадження та супроводження проектів з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

РН 20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної

	<p>безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.</p> <p>РН 21. Використовувати методи натурального, фізичного і комп'ютерного моделювання з метою детального вивчення і дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.</p> <p>РН 22. Планувати та виконувати експериментальні і теоретичні дослідження, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати адекватність результатів досліджень, аргументувати висновки.</p> <p>РН 23. 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.</p> <p>РН 24. Мати навички керування, розроблення, впровадження та супроводження проектів з забезпечення інформаційної безпеки та/або кібербезпеки.</p>
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	<p>Кадрове забезпечення ОПП формується, в основному за рахунок кафедри менеджменту та безпеки інформаційних систем. До викладання дисциплін залучаються також інші кафедри факультету менеджменту та безпеки інформаційних систем, і університету. Керівник проектної групи освітньої програми та викладацький склад, який забезпечує її реалізацію, відповідають вимогам, визначеним Ліцензійними умовами провадження освітньої діяльності.</p>
Матеріально-технічне забезпечення	<p>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.</p>

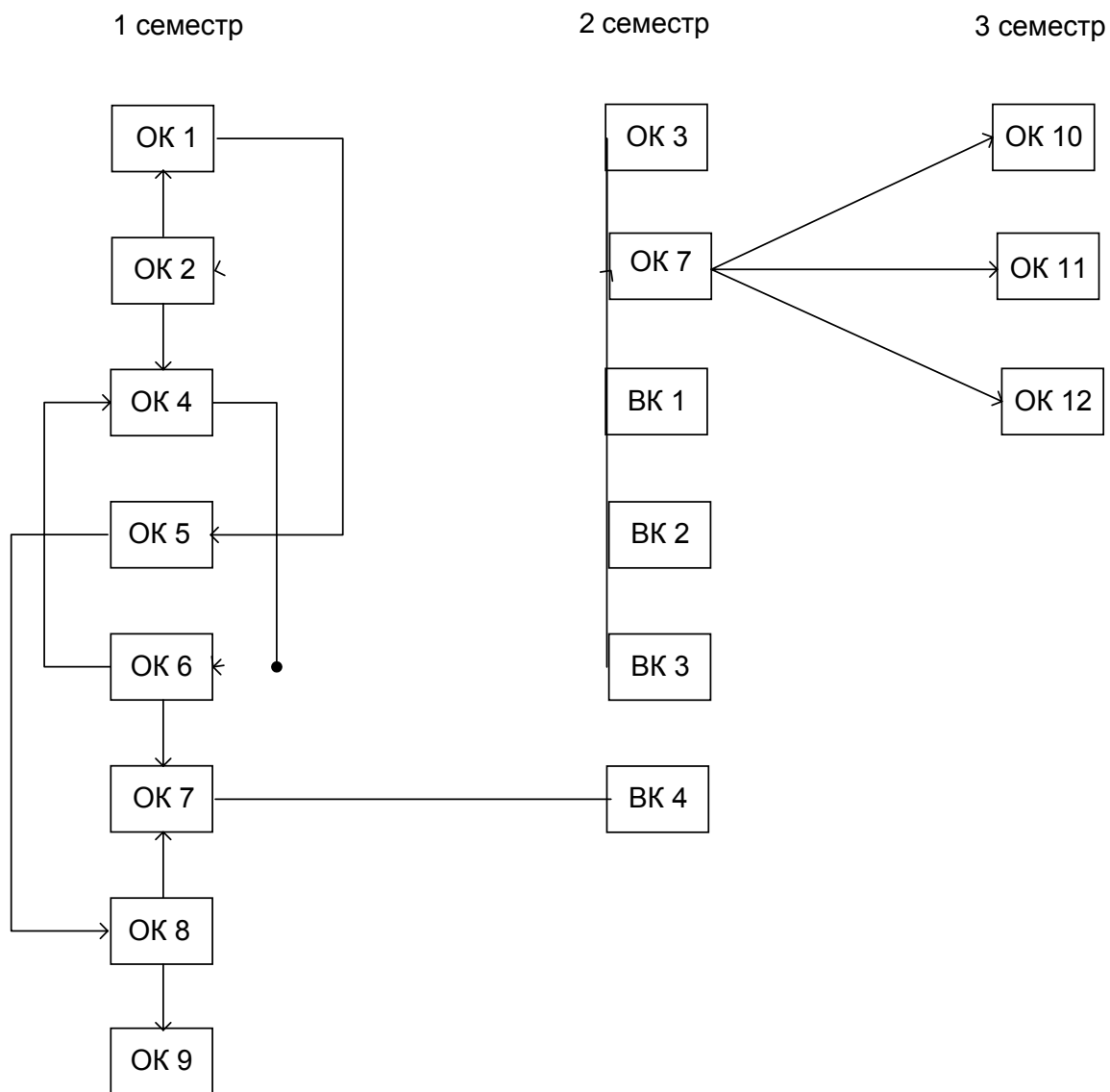
Інформаційне та навчально-методичне забезпечення	Відповідно до вимог Ліцензійних умов провадження освітньої діяльності включає в себе бібліотечні ресурси, електронні навчальні ресурси, сайт ВНТУ та сайт кафедри, на яких розміщена основна інформація щодо освітньої діяльності за ОП.
9 – Академічна мобільність	
Національна кредитна мобільність	Здійснюється на підставі укладення угод про співробітництво між Університетом та вищими навчальними закладами України.
Міжнародна кредитна мобільність	Здійснюється на підставі укладення угод між Університетом та групою вищих навчальних закладів 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.
Навчання іноземних здобувачів вищої освіти	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
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ			
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.	Економічне обґрунтування інноваційних рішень в інформаційних технологіях	4,0	залік
1.5.	Методологія та організація наукових досліджень	3,0	іспит
1.6.	Сучасні інформаційні технології в кібербезпеці	3,0	іспит
1.7.	Кібербезпека	9,0	іспит
1.8.	Системний аналіз і технології підтримки прийняття рішень (в т. ч. курсова робота)	5,0	іспит
1.9.	Аудит інформаційної безпеки	4,0	іспит
1.10.	Переддипломна практика	9,0	залік
1.11.	Магістерська кваліфікаційна робота	20,0	
1.12.	Державний кваліфікаційний екзамен	1,0	
Загальний обсяг обов'язкових компонент		67	
ВИБІРКОВІ КОМПОНЕНТИ ЗА ВІЛЬНИМ ВИБОРОМ СТУДЕНТА			
2.1.	Дисципліна 1 (з переліку 1 дис. 5 кред.)	5,0	залік
2.2.	Дисципліна 2 (з переліку 1 дис. 6 кред.)	6,0	залік
2.3.	Дисципліна 3 (з переліку 1 дис. 6 кред.)	6,0	залік
2.4.	Дисципліна 4 (з переліку 1 дис. 6 кред.)	6,0	залік
		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 та атестаційного екзамену.

Вимоги до кваліфікаційної роботи

Кваліфікаційна робота має розв'язання наукової або науково-технічної задачі у галузі інформаційної безпеки та/або кібербезпеки, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Кваліфікаційна робота має бути розміщена на офіційному сайті ВНТУ.

Вимоги до атестаційного екзамену. Атестаційний екзамен має передбачати оцінювання обов'язкових результатів навчання, визначених освітньої програмою.

4 Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

У вищому навчальному закладі 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 ефективною системою 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 стандарт вищої освіти

- 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 04.10.2018р.;
- «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 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 (компетентностей) та освітніх компонентів.

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

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 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				+	+							

**Таблиця 2. Матриця відповідності компетентностей
обов'язковим освітнім компонентам**

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12
ЗК 1						+	+	+	+	+	+	+
ЗК 2					+							
ЗК 3	+	+		+		+						
ЗК 4			+									
ЗК 5				+	+			+	+			
ЗК 6	+	+						+				
ЗК 7									+			
ЗК 8	+	+	+	+	+			+	+			
СК 1						+						
СК 2									+			
СК 3						+	+		+			
СК 4							+		+			
СК 5									+			
СК 6						+						
СК 7							+		+			
СК 8					+	+	+					
СК 9									+			
СК 10		+			+							