МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

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

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

Безпека інформаційних і комунікаційних систем
Information and Communications Systems Security

Рівень вищої освіти	перший (бакалаврський)
Спеціальність	125 Кібербезпека та захист інформації
Галузь знань	12 Інформаційні технології
Освітня кваліфікація	бакалавр з кібербезпеки та захисту інформації

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

.

Вінниця, 2023

ЛИСТ ПОГОДЖЕННЯ

ОПП Безпека інформаційних і комунікаційних систем

Рівень вищої освіти перший (бакалаврський)

Спеціальність 125 Кібербезпека та захист інформації

Гарант ОПП

к.т.н., доцент, доцент кафедри ЗІ _____ Леонід КУПЕРШТЕЙН

Директор Центру забезпечення

якості освіти ВНТУ _____ Олеся ВОЙТОВИЧ

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

протокол № 6 від 17 грудня 2022 р.

Зав. кафедри _____ Володимир ЛУЖЕЦЬКИЙ

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

засіданні Вченої ради факультету інформаційних технологій та комп'ютерної інженерії;

протокол №5 від 17 січня 2023 р.

Голова _____ Світлана КИРИЛАЩУК

засіданні Методичної ради ВНТУ,

протокол №6 від 19 січня 2023 р.

Голова _____ Олександр ПЕТРОВ

ПРЕАМБУЛА

ОПП Безпека інформаційних і комунікаційних систем

Рівень вищої освіти перший (бакалаврський)

Спеціальність 125 Кібербезпека та захист інформації

Розроблена на основі стандарту вищої освіти (наказ № 1074 від 04.10.2018 р. «Про затвердження стандарту вищої освіти зі спеціальності 125 Кібербезпека для першого (бакалаврського) рівня вищої освіти»)

РОЗРОБНИКИ

Гарант ОПП, доцент кафедри захисту інформації, к.т.н., доцент	Леонід КУПЕРШТЕЙН
доцент кафедри захисту інформації, к.т.н., доцент	Юрій БАРИШЕВ
доцент кафедри захисту інформації, к.т.н., доцент	Віталій ЛУКІЧОВ
завідувач кафедри захисту інформації, д.т.н., професор	Володимир ЛУЖЕЦЬКИЙ

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

протокол № 10 від 13.01.2023 р.

Голова  Аліна ВОВКОВИНСЬКА

РЕЦЕНЗІЇ-ВІДГУКИ РОБОТОДАВЦІВ

На освітньо-професійну програму надіслали рецензії та відгуки:

Олександр Ульяненков, підполковник поліції, начальник Управління протидії кіберзлочинам у Вінницькій області

Вадим Груша, директор ТОВ «Trustee Global»

Сергій Іванченко, д.т.н., проф. ІСЗЗІ КПІ ім. Ігоря Сікорського

Володимир Романенко, директор департаменту інформаційних технологій Вінницької міської ради

ВСТУП

Освітньо-професійна програма (далі – ОПП) підготовки бакалаврів зі спеціальністю 125 Кібербезпека та захист інформації розроблена на основі стандарту з вищої освіти зі спеціальності 125 Кібербезпека першого (бакалаврського) рівня вищої освіти затвердженого Наказом МОН України №1074 від 4.10.18.

1 ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Вінницький національний технічний університет, кафедра захисту інформації
Ступінь вищої освіти та назва освітньої кваліфікації мовою оригіналу	Бакалавр Бакалавр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Безпека інформаційних і комунікаційних систем
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний На базі ПСЗО - 240 кредитів ЄКТС, термін навчання – 3 роки 10 місяців.
Кваліфікація в дипломі	Ступінь вищої освіти – Бакалавр Спеціальність –125 Кібербезпека та захист інформації Освітня програма – Безпека інформаційних і комунікаційних систем
Цикл/рівень	6 рівень НРК України, перший цикл FQ-EHEA, 6 рівень EQF-LLL
Передумови	Повна загальна середня освіта
Мова (и) викладання	Українська, за потреби один або декілька освітніх компонентів можуть викладатися англійською мовою
Акредитація	Сертифікат про акредитацію ОПП УД 02005339 терміном дії до 01.07.2023
Інтернет-адреса постійного розміщення опису освітньої програми	http://vntu.edu.ua/uk/information-for-enrollee/progmagbak.html
2 – Мета освітньої програми	
Формування творчої особистості нового покоління, здатної успішно реалізовувати набуті сучасні професійні компетентності з безпеки інформаційних і комунікаційних систем, інтелектуальний потенціал, навики практичного досвіду та інноваційної діяльності в галузі кібербезпеки та захисту інформації, а також соціально-патріотичні та морально-етичні цінності у глобальному суспільно-економічному просторі[1]	

3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація	Галузь знань – 12 Інформаційні технології Спеціальність – 125 Кібербезпека та захист інформації
Об’єкти професійної діяльності випускників	- об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту
Цілі навчання	підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки
Теоретичний зміст предметної області. Знання	- законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування.
Методи, методики та технології	Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки
Інструменти та обладнання	Системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Основний фокус освітньої програми та спеціалізації	Загальна – діяльність із забезпечення інформаційної та/або кібербезпеки. Спеціальна – діяльність із забезпечення інформаційної та/або кібербезпеки у інформаційних і комунікаційних системах. Ключові слова: інформаційна безпека, кібербезпека,

	захист інформації
Особливості програми	Мінімум 75% обсягу освітньої програми має бути спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю визначеною стандартом вищої освіти. ОПП спрямована на забезпечення інформаційної та/або кібербезпеки у інформаційних та комунікаційних системах, що використовуються у підприємствах та організаціях різної форми власності.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Професійна діяльність за такими назвами робіт: 3439 Фахівець із організації інформаційної безпеки, Фахівець із організації захисту інформації з обмеженим доступом відповідно Класифікатора професій ДК 003:2010. Права випускників на працевлаштування не обмежуються.
Подальше навчання	Мають право продовжити навчання на другому (магістерському) рівні вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Лекції, практичні заняття, виконання курсових робіт/проектів, лабораторні роботи, самостійна робота на основі підручників, навчальних посібників та конспектів лекцій, інформаційних ресурсах, консультації із викладачами, семінари, демонстраційні класи, елементи дистанційного (онлайн, електронного) навчання проходження практики на профільних підприємствах та в науково-дослідних установах, підготовка кваліфікаційної роботи.
Оцінювання	Методи оцінювання – екзамени, диференційовані заліки, заліки, тести, практика, контрольні, курсові роботи/проекти, 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, диф.залік/залік (за результатами формативного контролю).
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності	КЗ1. Здатність застосовувати знання у практичних ситуаціях.

	КЗ2. Знання та розуміння предметної області та розуміння професії. КЗ3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. КЗ4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ5. Здатність до пошуку, оброблення та аналізу інформації. КЗ6.Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. КЗ7.Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області,її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Фахові компетентності	КФ1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. К6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих)систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження. КФ7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту

	інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) КФ8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. КФ11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
7 – Програмні результати навчання	
РН01. застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН02. організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН03. використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН04. аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН05. адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН06. критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН07. діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН08. готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН09. впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН10. виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;	

РН11. виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах;
РН12. розробляти моделі загроз та порушника;
РН13. аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;
РН14. вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;
РН15. використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;
РН16. реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;
РН17. забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) системна основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі,сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент
РН18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;
РН19. застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
РН20. забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;
РН21. вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
РН22. вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;
РН23. реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
РН24. вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);
РН25. забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;
РН26. впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) системна основі еталонної моделі взаємодії відкритих систем;
РН27. вирішувати задачі захисту потоків даних в інформаційних, інформаційно-

телекомунікаційних (автоматизованих) системах;
РН28. аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки;
РН29. здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;
РН30. здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
РН31. застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
РН32. вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки
РН33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;
РН34. приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;
РН35. вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;
РН36. виявляти небезпечні сигнали технічних засобів;
РН37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;
РН38. інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;
РН39. проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;
РН40. інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;
РН41. забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;
РН42. впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;
РН43. застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;
РН44. вирішувати задачі забезпечення безперервності бізнес-процесів організації на

основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН45. застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН46. здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН47. вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН48. виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН49. забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН50. забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН51. підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН52. використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; РН53. вирішувати задачі аналізу програмного коду на наявність можливих загроз. РН54. усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.	
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Кадрове забезпечення ОПП формується, в основному за рахунок кафедри захисту інформації. До викладання дисциплін залучаються також інші кафедри університету. Група забезпечення та гарант освітньої програми, які забезпечують її реалізацію, відповідають вимогам, визначеним Ліцензійними умовами провадження освітньої діяльності та іншим нормативним документам.
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення відповідає вимогам Ліцензійних умов провадження освітньої діяльності, в тому числі включає в себе спеціалізовані лабораторії (захисту програмного забезпечення, технічного захисту інформації, захисту комп'ютерних мереж), направлені на здобуття спеціальних (фахових) компетентностей, оволодіння практичним навичками забезпечення кібербезпеки, зокрема безпеки інформаційних і комунікаційних систем, а також інші спеціалізовані лабораторії ВНТУ
Інформаційне та навчально-методичне забезпечення	Включає в себе бібліотечні ресурси, систему підтримки освітнього процесу JetIQ, електронні навчальні ресурси, сайт ВНТУ та сайт кафедри, на яких розміщена основна

	інформація щодо освітньої діяльності за ОПП.
9 – Академічна мобільність	
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 закладами 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 ВНТУ приймає 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

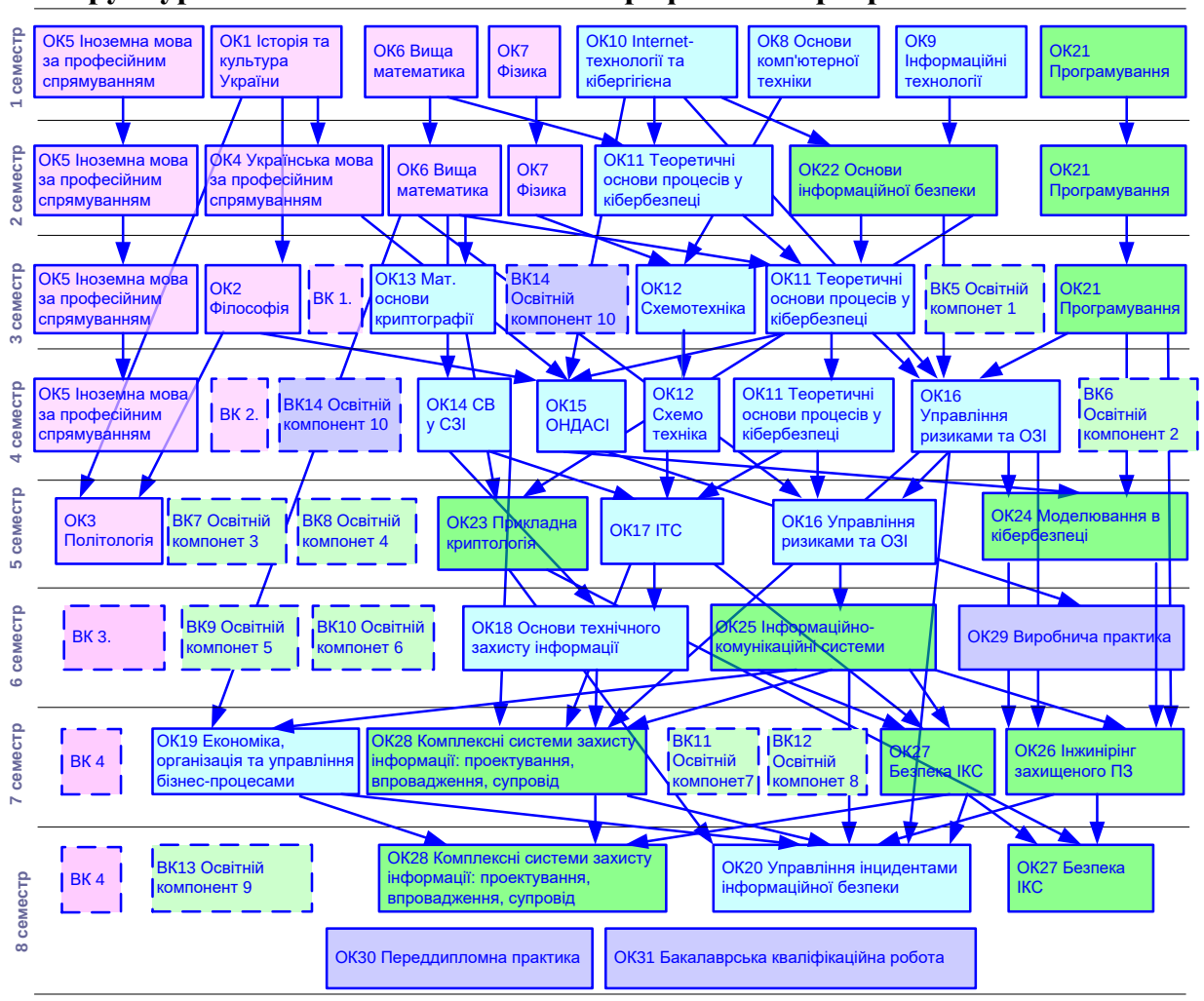
Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов’язкові компоненти ОП			
Загальні			
ОК 1.	Історія та культура України	3,0	залік
ОК 2.	Філософія	3,0	залік
ОК 3.	Політологія *	3,0	залік
ОК 4.	Українська мова за професійним спрямуванням *	3,0	залік
ОК 5.	Іноземна мова за професійним спрямуванням *	8,0	залік
ОК 6.	Вища математика	12,0	іспит
ОК 7.	Фізика	10,0	іспит
Професійні			
ОК 8.	Основи комп'ютерної техніки	3,0	іспит
ОК 9.	Інформаційні технології	3,0	залік
ОК 10.	Internet-технології та кібергігієна	4,0	іспит
ОК 11.	Теоретичні основи процесів у кібербезпеці	11,0	іспит
ОК 12.	Схемотехніка	8,0	іспит
ОК 13.	Математичні основи криптографії	4,0	іспит
ОК 14.	Спеціальні вимірювання у сфері захисту інформації	3,0	залік
ОК 15.	Основи наукових досліджень, аналізу та синтезу інформації	4,0	іспит
ОК 16.	Управління ризиками та оцінювання захищеності інформації	6,0	іспит
ОК 17.	Інформаційно-телекомунікаційні системи	3,0	іспит
ОК 18.	Основи технічного захисту інформації	5,0	іспит
ОК 19.	Економіка, організація та управління бізнес-процесами	3,0	залік
ОК 20.	Управління інцидентами інформаційної безпеки	4,0	іспит
ОК 21.	Програмування (в т.ч. курсова робота)	15,0	іспит

ОК 22.	Основи інформаційної безпеки	3,0	іспит
ОК 23.	Прикладна криптологія (в т.ч. курсова робота)	6,0	іспит
ОК 24.	Моделювання в кібербезпеці	5,0	іспит
ОК 25.	Інформаційно-комунікаційні системи	3,0	іспит
ОК 26.	Інжинірінг захищеного програмного забезпечення (в т.ч. курсова робота)	5,0	іспит
ОК 27.	Безпека інформаційно-комунікаційних систем (в т.ч. курсовий проект)	8,0	іспит
ОК 28.	Комплексні системи захисту інформації: проектування, впровадження, супровід (в т.ч. курсова робота)	8,0	іспит
ОК 29.	Виробнича практика	9,0	залік
ОК 30.	Переддипломна практика	4,5	залік
ОК 31.	Бакалаврська кваліфікаційна робота	10,5	захист
Загальний обсяг обов'язкових компонентів:		**180**	
2. ВИБІРКОВІ КОМПОНЕНТИ ОП ЗА ВІЛЬНИМ ВИБОРОМ СТУДЕНТА			
Загальні			
ВК 1.	Освітній компонент з гуманітарної та філософської підготовки з БДВВ	3,0	залік
ВК 2.	Освітній компонент з суспільно-політичної підготовки з БДВВ	3,0	залік
ВК 3.	Освітній компонент з економічної підготовки / менеджменту / підприємництва та управління проектами з БДВВ	3,0	залік
ВК 4.	Освітній компонент підготовки з іноземної мови з БДВВ	3,0	залік
Професійні			
ВК 5	Освітній компонент 1 з БДВВ**	5,0	залік
ВК 6	Освітній компонент 2 з БДВВ	5,0	залік
ВК 7	Освітній компонент 3 з БДВВ	5,0	залік
ВК 8	Освітній компонент 4 з БДВВ	5,0	залік
ВК 9	Освітній компонент 5 з БДВВ	5,0	залік
ВК 10	Освітній компонент 6 з БДВВ	5,0	залік
ВК 11	Освітній компонент 7 з БДВВ	6,0	залік
ВК 12	Освітній компонент 8 з БДВВ	5,0	залік
ВК 13	Освітній компонент 9 з БДВВ	3,0	залік
ВК 14	Освітній компонент 10 з БДВВ	4,0	залік
Загальний обсяг вибіркових компонентів:		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

* Українська мова як іноземна (14 кредитів) для іноземців та осіб без громадянства

** БДВВ – база дисциплін вільного вибору

2.2. Структурно-логічна схема освітньо-професійної програми



3 ФОРМИ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форми атестації здобувачів вищої освіти

Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту та публічного захисту кваліфікаційної роботи.

До атестації допускаються студенти, які виконали всі вимоги програми підготовки.

Вимоги єдиного державного кваліфікаційного іспиту

Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом та освітньою програмою.

Вимоги до кваліфікаційної роботи

Кваліфікаційна робота має передбачати розв’язання спеціалізованої задачі в галузі інформаційної та/або кібербезпеки.

Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації.

Кваліфікаційна робота має бути розміщена на офіційному сайті ВНТУ (репозитарії) у системі JetIQ.

4 ХАРАКТЕРИСТИКА СИСТЕМИ ВНУТРІШНЬОГО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ПІДГОТОВКИ БАКАЛАВРА

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 та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті ВНТУ, 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 чи спеціальністю;

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 і здобувачів вищої освіти;

9) інших процедур і заходів.

5 ПЕРЕЛІК НОРМАТИВНИХ ДОКУМЕНТІВ, НА ЯКИХ БАЗУЄТЬСЯ ОСВІТНЯ ПРОГРАМА

1. Закон України «Про вищу освіту» 01.07.2014 No1556-VII - Режим доступу: http://zakon4.rada.gov.ua/laws/show/1556-18.

2. Закон України «Про захист інформації в інформаційно-телекому-нікаційних системах» - відомості Верховної Ради України (ВВР), 1994, N 31, ст.286.

3.Закон України "Про основні засади забезпечення кібербезпеки України"- відомості Верховної Ради (ВВР), 2017, № 45, ст.403.

4.«Доктрина інформаційної безпеки України», затверджено Указом Президента України від 25 лютого 2017 року № 47/2017.

5.Постанова Кабінету Міністрів «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 29.04.2015 р. № 266.

6.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.

7.Постанова Кабінету Міністрів «Про затвердження Ліцензійних умов провадження освітньої діяльності» від 30.12.2015 №1187.

8. Наказ МОН України No166 «Деякі питання оприлюднення інформації про діяльність вищих навчальних закладів» від 19.02.2015 р.

9. Наказ МОН України «Про особливості запровадження переліку галузей знань, за якими здійснюється підготовка здобувачів вищої освіти, затвердженого постановою КМУ від 29.04. 2015 р.» № 266 від 06.11.2015 р.

10. Національний класифікатор України: "Класифікатор професій" ДК 003:2010 // Видавництво "Соцінформ". -К.: 2010.

11. Наказ Міністерства економічного розвитку і торгівлі України «Про затвердження зміни до національного класифікатора України ДК 003:2010» від 18.11.2014 р. №1361 (зміна № 2).

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

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

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

Освітньо-професійна програма містить програмні компетентності, що визначають специфіку підготовки бакалаврів зі спеціальності 125 Кібербезпека та захист інформації та програмні результати навчання, які відображають те, що студент повинен знати, розуміти та бути здатним виконувати після успішного завершення освітньої програми. В таблицях 1, 2 наведені матриці відповідності визначених освітньою програмою результатів навчання (компетентностей) та освітніх компонентів розроблені на основі додатку №1 стандарту вищої освіти.

Додаток №1

Фахові компетентності	Результати навчання
КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.	- готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки; - розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем; - виконувати аналіз реалізації прийнятої політики інформаційної і /або кібербезпеки.

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.	- здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; - розробляти та аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; - застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем,методів і засобів обробки інформації, архітектур операційних систем; - здійснювати захист ресурсів і процесів в інформаційно-телекомунікаційних системах на основі моделей безпеки (кінцевих автоматів, управління потоками, Bell-LaPadula, Biba, Clark-Wilson, та інші), а також встановлених режимів безпечного функціонування інформаційно-телекомунікаційних системах; - виконувати аналіз програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної і\або кібербезпеки в інформаційно-телекомунікаційних системах.
КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах	- забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; - забезпечувати функціонування спеціального програмного забезпечення,щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - виконувати розробку експлуатаційної документації на комплексів засобів захисту.
КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.	- вирішувати задачі супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); - вирішувати задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - забезпечувати введення підзвітності системи

	управління доступом інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	- обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної та/або кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації; - вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах-проектувати та реалізувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації; - вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.	- вирішувати задачі управління процесами забезпечення безперервності бізнесу з використанням процедур резервування програмного забезпечення та безпосередньо інформаційних ресурсів; - вирішувати задачі корекції цілей, стратегій, планів забезпечення безперервності бізнес процесів після здійснення кібератак, збоїв та відмов різних класів. - створювати і впроваджувати плани процесу забезпечення безперервності бізнесу; - виконувати аналіз налаштувань елементів інформаційних систем та комунікаційного обладнання.
КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)	- вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - здійснювати оцінку рівня захищеності інформації що обробляється в інформаційно-телекомунікаційних системах використовувати інструментальні засоби оцінювання наявності потенційних вразливостей; - вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих); - вирішувати задачі експертизи, випробування комплексних систем захисту інформації.
КФ 8. Здатність здійснювати	- вирішувати задачі попередження та виявлення,

процедури управління інцидентами, проводити розслідування, надавати їм оцінку.	ідентифікації, аналізу та реагування на інциденти в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - проводити розслідування інцидентів інформаційної безпеки та/або кібербезпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної безпеки та/або кібербезпеки; - забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації.
КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.	- забезпечувати безперервність бізнес процесів організації на базі теорії ризиків та системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів; - забезпечувати функціонування системи управління інформаційною та\або кібербезпекою організації на основі керування інформаційними ризиками, здійснення процедур їх кількісного і якісного оцінки.
КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.	- аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації; - аналізувати та визначати можливість застосування технологій, методів та засобів технічного захисту інформації; - виявляти небезпечні сигнали технічних засобів; - вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю захищеності інформації від витоку технічними каналами; - визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; - інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; - обґрунтовувати можливість створення технічних каналів витоку інформації на об’єктах інформаційної діяльності; - впроваджувати заходи та засоби технічного захисту інформації від витоку технічними каналами.
КФ 11. Здатність виконувати моніторинг ресурсів і процесів функціонування, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	- забезпечувати процеси моніторингу доступу до ресурсів і процесів інформаційно-телекомунікаційних систем; - забезпечувати конфігурування та функціонування систем моніторингу ресурсів та процесів в інформаційно-телекомунікаційних системах.

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно встановленої політики інформаційної та/або кібербезпеки.	- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в інформаційно-телекомунікаційних системах; - аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.

Додаток №2

Додаткова література

1.Payment Card Industry Data Security Standard (PCI DSSISO/IEC27001:2013).

2.ISO/IEC 27002:2012/16 Information technology. Security techniques. Code of practice for information security management–Інфорацій1ні технології. Стандарт.

3.ISO/IEC 27005:2011 Information security risk management —Управління ризиками інформаційної безпеки. Стандарт.

4.ISO/IEC 27032:2016Informationtechnology. «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности».

5.International Standard Classification of Occupations 2008, міжнародний класифікатор професій.

6.Розвиток системи забезпечення якості вищої освіти в Україні: інформаційно-аналітичний огляд, Національна академія педагогічних наук України, Інститут вищої освіти НАПН України. Режим доступу: http://ihed.org.ua/images/biblioteka/ Rozvitok_sisitemi_zabesp_yakosti_VO_UA_2015.pdf.

7.Розроблення освітніх програм: методичні рекомендації -Режим доступу: http://ihed.org.ua/images/biblioteka/rozroblennya_osv_program_2014_tempus-office.pdf.

8.Методичні рекомендації щодо розроблення стандартів вищої освіти.

9.Bragg R. Certified Information Systems Security Professional (CISSP, InternationalStandard).

10.Stewart J. M. SSCP Systems Security Certified Practitioner. – 2006.

11.CobiT C. Control Objectives for Information and related Technology //IT Governance Institute www. isaca. org. –2002.

12.Information technology – Security techniques–Information security management systems–Requirements. –2005.

13.Commissie E. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. –2013.

14.Індустріальні моделі Кібербезпеки США -3.2-2016, ETAUSD: Cybersecurity Industry Model: 2014. InternationalStandard.

15.«Біла книга Держспецзв'язку». Електронний ресурс. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=49942&cat_id=4994.

16.TUNING (для ознайомлення зі спеціальними (фаховими) компетентностями та прикладами стандартів. Електронний ресурс. – Режим доступу: http://www.unideusto.org/tuningeu.

.

Додаток Б

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	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31
РН 1				+	+																										
РН 2						+			+	+	+				+	+		+		+	+	+	+			+	+	+	+	+	+
РН 3							+		+	+	+				+	+	+		+	+	+	+	+			+	+	+	+	+	+
РН4		+	+			+			+	+	+				+	+		+	+	+		+	+		+	+	+	+	+	+	+
РН5								+	+	+	+	+	+		+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+
РН 6	+	+	+			+	+		+	+	+		+		+	+			+			+	+			+	+	+	+	+	+
РН7										+				+	+	+		+		+		+	+		+		+	+	+	+	+
РН8																												+			
РН9														+		+		+		+		+					+	+	+	+	
РН10								+	+		+						+								+		+				
РН 11									+	+							+								+		+				
РН12											+					+				+		+		+			+	+	+	+	
РН13								+									+								+		+				
РН14										+											+	+		+		+		+			
РН15										+		+					+				+		+		+	+	+				
РН16														+				+										+			
РН17								+		+	+	+					+										+				
РН18										+				+									+			+	+				
РН19																							+	+		+		+	+	+	+
РН20										+																+	+	+			
РН21																												+			
РН22										+												+	+	+		+	+				
РН23																				+			+			+		+			
РН24											+											+		+			+	+			
РН25																				+											
РН26																	+							+	+			+			
РН27										+													+	+			+	+			
РН28																+								+				+			
РН29																+						+		+				+			
РН30																+	+	+				+	+					+	+		
РН31														+									+	+				+	+	+	+
РН32								+		+							+					+					+	+			
РН33																+			+	+											
РН34																						+						+			
РН35														+														+			
РН36											+	+		+				+													
РН37												+		+				+													
РН38														+				+													

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31
РН39																		+										+			
РН40														+				+													
РН41																				+											
РН 42																		+		+											
РН 43																		+		+											
РН 44																+			+	+											
РН45																+				+											
РН46																+															
РН47													+										+				+	+			
РН48											+		+										+				+	+			
РН49																	+			+								+			
РН50											+															+	+				
РН51																				+							+				
РН52																	+			+							+	+			
РН53																					+					+	+				
РН54	+	+	+							+					+				+												

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	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31
К31		+	+			+			+	+	+				+	+		+	+	+		+	+		+	+	+	+	+	+	+
К32								+	+	+	+	+	+		+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+
К33				+	+																										
К34						+			+	+	+				+	+		+		+	+	+	+			+	+	+	+	+	+
К35	+	+	+			+	+		+	+	+		+		+	+	+		+	+	+	+	+			+	+	+	+	+	+
К36	+	+	+							+					+				+												
К37	+	+	+				+								+				+												
КФ1										+				+	+	+		+		+		+	+		+		+	+	+	+	+
КФ2								+	+	+	+	+					+					+		+	+		+	+			
КФ3										+		+		+			+				+	+	+	+	+	+	+	+	+	+	+
КФ4																	+			+		+	+	+	+	+		+			
КФ5										+						+	+					+	+	+		+	+	+	+	+	+
КФ6								+		+							+					+						+	+		
КФ7												+		+				+											+			
КФ8																		+		+												
КФ9																+			+	+												
КФ10											+	+	+	+				+					+				+	+				
КФ11											+						+			+						+	+	+				
КФ12																+		+		+	+	+				+	+	+	+	+		

ЛИСТОК РЕЄСТРАЦІЇ ЗМІН

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