МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Системи технічного захисту інформації, автоматизація її обробки»

БАКАЛАВР (перший рівень освіти)

за спеціальністю	125 Кібербезпека
галузь знань	12 Інформаційні технології
кваліфікація	3439 Фахівець із організації захисту інформації з обмеженим доступом
спеціалізація	Системи технічного захисту інформації, автоматизація її обробки

ЗАТВЕРДЖЕНО
ВЧЕНОЮ РАДОЮ ЗНТУ
Голова вченої ради
Ректор ЗНТУ
_____/Бєліков С.Б./
(протокол № __ від «__» _____ 2019 р.)
Освітня програма вводиться в дію з 01.09.2019 р.
Ректор ЗНТУ_____/С.Б. Бєліков/
(наказ № __ від «__» _____ 2019 р.

Запоріжжя 2019

ЛИСТ ПОГОДЖЕННЯ

Освітньо-професійної програми

БАКАЛАВР (перший рівень освіти)

Спеціальність	125 Кібербезпека
Галузь знань	12 Інформаційні технології
кваліфікація	3439 Фахівець із організації захисту інформації з обмеженим доступом
спеціалізація	Системи технічного захисту інформації, автоматизація її обробки

Розробники програми:

1. **Воскобойник В.О.** – канд. техн. наук, доцент
2. **Неласа Г.В.** – канд. техн. наук, доцент
3. **Романенко С.М.** – канд. фіз.-мат. наук, доцент

ВНЕСЕНО
Кафедрою «Захист інформації»
Протокол № __ від «___» _____ 201_ р.
Завідувач кафедри _____ Карпуков Л.М.
ПОГОДЖЕНО
Вченою радою факультету радіоелектроніки і телекомунікацій
Протокол № __ від « __» _____ 201_ р.
Голова вченої ради факультету _____ Кабак В.С.
СХВАЛЕНО
Науково-методичною комісією факультету
Протокол № __ від « __ » _____ 201_ р.
Голова НМК факультету _____ Кабак В.С.
НАДАНО ЧИННОСТІ ТА ВВЕДЕНО У ДІЮ
Наказ ЗНТУ № __ від « __» _____ 201_ р.

ПЕРЕДМОВА

Освітньо-професійна програма (ОПП) розроблена на підставі *Стандарту вищої освіти* першого (бакалаврського) рівня. Галузь знань 12 Інформаційні технології. Спеціальність 125 Кібербезпека. Затверджено і введено в дію наказом МОН України від 04.10.2018 р. № 1074.

ОПП розроблена робочою групою (науково-методичною комісією спеціальності 125 Кібербезпека) у складі:

1. **Воскобойник Володимир Олександрович** – член проектної групи, кандидат технічних наук, доцент кафедри захисту інформації Запорізького національного технічного університету;
2. **Неласа Ганна Вікторівна** – член проектної групи, кандидат технічних наук, доцент кафедри захисту інформації Запорізького національного технічного університету.
3. **Романенко Сергій Миколайович** – член проектної групи, кандидат фізико-математичних наук, доцент кафедри захисту інформації Запорізького національного технічного університету.

1. Профіль освітньої програми зі спеціальності 125 «Кібербезпека» (за спеціалізацією «Системи технічного захисту інформації, автоматизація її обробки»)

1-Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Запорізький національний технічний університет Кафедра «Захист інформації»
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь вищої освіти – бакалавр. Кваліфікація: 3439 Фахівець із організації захисту інформації з обмеженим доступом
Офіційна назва освітньої програми	Освітньо-професійна програма «Системи технічного захисту інформації, автоматизація її обробки» першого рівня вищої освіти за спеціальністю 125 «Кібербезпека»
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС термін навчання 4 роки
Наявність акредитації	Нац. агентство забезпечення якості вищої освіти. Україна. Термін подання програми на акредитацію – 2019 р.
Цикл/рівень	НРК України – 7 рівень, QF-ENEA – перший цикл, EQF - LLL – 6 рівень
Передумови	Наявність повної загальної середньої освіти.
Мова викладання	Українська
Термін дії освітньої програми	31.05.2024 р.
Інтернет – адреса постійного розміщення опису освітньої програми	http://www.zntu.edu.ua/
2 – Мета освітньої програми	
Формування особистості фахівця, здатного вирішувати типові та складні завдання забезпечення захисту ресурсів від загроз конфіденційності, цілісності, доступності у кіберпросторі, забезпечити умови формування	

бакалаврами програмних компетентностей, що дозволять їм оволодіти основними знаннями та навичками для подальшої професійної діяльності.	
3-Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація)	Галузь знань 12 «Інформаційні технології» Спеціальність 125 «Кібербезпека» Спеціалізація «Системи технічного захисту інформації, автоматизація її обробки»
Орієнтація освітньої програми	Освітньо-професійна програма пропонує комплексний підхід до вирішення сучасних проблем в сфері захисту інформації з обмеженим доступом; враховує специфіку роботи організацій, установ та підприємств у вказаній сфері; дозволяє отримати необхідні навички в галузі забезпечення захищеності об'єктів інформатизації різного рівня.
Основний фокус освітньої програми	Формування компетентностей для здійснення діяльності у сфері захисту інформації з обмеженим доступом. Акцент на здатність розробки нових проектних рішень, на розвиток ефективних навичок комплексного підходу під час вирішення поставлених завдань у фаховій галузі.
Особливості програми	Програма зорієнтована на підготовку фахівців, діяльність яких пов'язана з забезпеченням захисту інформації з обмеженим доступом.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Сферою працевлаштування випускників є підприємства, організації, установи різного рівня та форм власності. Види економічної діяльності (за КВЕД ДК 009:2010): 61.1 Діяльність у сфері дротового електрозв'язку. 61.2 Діяльність у сфері бездротового електрозв'язку. 61.3 Діяльність у сфері супутникового електрозв'язку. 61.9 Інша діяльність у сфері електрозв'язку. 62.09 Інша діяльність у сфері інформаційних технологій і комп'ютерних систем. 63.1 Оброблення даних, розміщення інформації на веб-вузлах і пов'язана з ними діяльність; веб-портали. 80.1 Діяльність приватних охоронних служб. 80.2 Обслуговування систем безпеки. 84.22 Діяльність у сфері оборони. Фахівець з безпеки інформаційних і комунікаційних систем може займати первинні посади згідно з Національним класифікатором України «Класифікатор професій» ДК 003:2010(зі змінами):

	3121 Фахівець з інформаційних технологій. 3439 Фахівець з режиму секретності. 3439 Фахівець із організації захисту інформації з обмеженим доступом. 3439 Фахівець із організації інформаційної безпеки.
Подальше навчання	Право вступу на навчання за освітньо-кваліфікаційним рівнем «магістр» відповідно до напряму /восьмий кваліфікаційний рівень НРК.
5 – Викладання та оцінювання	
Викладання та навчання	Освітньо-професійною програмою передбачено використання інноваційних підходів (студенто-центрованого, індивідуалізованого, кооперативного, проблемного тощо), технологій (структурно-логічних, інтеграційних, інформаційно-комп'ютер-них, діалогово-комунікаційних тощо) і методів навчання (пояснювально-ілюстративного, репродуктивного, евристичного, проблемного викладання тощо). Викладання проводиться у вигляді: лекцій, семінарів, практичних занять, лабораторних робіт, самостійного навчання на основі підручників та конспектів, підготовки курсових робіт та проектів.
Оцінювання	Оцінювання навчальних досягнень здійснюється за 100-бальною (рейтинговою) шкалою ЕКТС (ECTS), національною 4-ри бальною шкалою («відмінно», «добре», «задовільно», «незадовільно») і вербальною («зараховано», «не зараховано») системами. *Види контролю*: поточний, рубіжний, тематичний, підсумковий, самоконтроль. *Форми контролю*: усні та письмові екзамени, диференційні заліки, тестові завдання, графічні роботи, перегляди, захист курсових робіт та проектів, звітів з практик, кваліфікаційний екзамен.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані завдання та практичні проблеми в галузі інформаційної та/або кібербезпеки або в процесі навчання, що передбачає застосування певних теорій та методів відповідної науки і характеризується комплексністю та невизначеністю умов.
Загальні компетентності (КЗ)	КЗ 1. Здатність застосовувати знання в практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 3. Здатність професійно спілкуватися державною та

	іноземною мовами як усно, так і письмово. КЗ 4. Вміти виявляти, ставити та вирішувати проблеми за професійним спрямуванням, здійснювати професійну діяльність на основі техніко-економічного аналізу. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КЗ 6. 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. КЗ 7. 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. КЗ 8. Здатність використовувати знання базових розділів фізики і математики в обсязі, необхідному для засвоєння фахових дисциплін. КЗ 9. Здатність приймати обґрунтовані рішення. КЗ 10. Здатність до адаптації та дії в новій ситуації.
Фахові компетентності спеціальності (КФ)	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. КФ 2. Здатність впроваджувати принципи організаційного забезпечення і порядок формування політики безпеки на об'єктах інформаційної діяльності. КФ 3. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки. КФ 4. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах КФ 5. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

	КФ 6. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах, з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 7. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 8. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) КФ 9. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 10. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 11. Здатність застосовувати методи та засоби криптографічного, стеганографічного та технічного захисту інформації на об’єктах інформаційної діяльності. КФ 12. Здатність виконувати моніторинг ресурсів і процесів функціонування, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 13. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно встановленої політики інформаційної та/або кібербезпеки. КФ 14. Здатність здійснювати проектування (розробку) пристроїв, систем, технологій і засобів інформаційної безпеки. КФ 15. Здатність здійснювати професійну діяльність згідно з вимогами санітарно-гігієнічного режиму, охорони праці, техніки безпеки та протипожежної безпеки.

7 – Програмні результати навчання (ПРН)	
Загальні програмні результати навчання	ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. ПРН 3. Використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. ПРН 4. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. ПРН 5. 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. ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності, що базуються на культурно-історичних, світоглядних та державницьких аспектах. ПРН 7. Аналізувати економічну ефективність заходів інформаційної безпеки, застосовувати основні засади охорони праці та безпеки життєдіяльності. ПРН 8. Використовувати знання про фізичні явища та володіти математичним апаратом для моделювання об'єктів інформаційної діяльності. ПРН 9. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. ПРН 10. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ПРН 11. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

Фахові програмні результати навчання	ПРН 12. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. ПРН 13. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. ПРН 14. Розробляти моделі загроз та порушника. ПРН 15. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних. ПРН 16. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень. ПРН 17. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. ПРН 18. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів. ПРН 19. Забезпечувати процеси захисту та функціонування інформаційно- телекомунікаційних (автоматизованих) систем на 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. ПРН 20. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах. ПРН 21. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах. ПРН 22. 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.

	ПРН 23. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно- телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки. ПРН 24. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ПРН 25. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових). ПРН 26. 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. ПРН 27. 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. ПРН 28. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. ПРН 29. 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. ПРН 30. Виявляти небезпечні сигнали технічних засобів. ПРН 31. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. ПРН 32. 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. ПРН 33. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних

	системах з використанням сучасних методів та засобів криптографічного та стеганографічного захисту інформації. ПРН 34. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). ПРН 35. Вирішувати задачі аналізу програмного коду на наявність можливих загроз. ПРН 36. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Викладачі, які забезпечують підготовку бакалаврів за спеціальністю 125 «Кібербезпека» мають науковий ступінь та вчене звання за відповідною або спорідненою спеціальністю, систематично займаються науковою і навчально-методичною діяльністю, регулярно проходять стажування, їх базова освіта відповідає профілю дисциплін, які вони викладають в ЗНТУ.
Матеріально - технічне забезпечення	Лекційні, аудиторні приміщення, спеціалізовані лабораторії, мультимедійне обладнання відповідно до вимог навчального процесу. Всі комп'ютери об'єднані у локальну мережу, в якій виділені домени (підмережі) для різних аудиторій і за призначенням: навчальний процес, наука, системно-технічні потреби. Університет має доступ до волоконно-оптичної мережі Уран. Для входу до локальної мережі та мережі Internet, крім того, встановлено Wi-Fi точки доступу. Для проведення інформаційного пошуку та обробка результатів є спеціалізовані комп'ютерні класи кафедри та університету, де наявне спеціалізоване програмне забезпечення та необмежений відкритий доступ до мережі Інтернет.
Інформаційне та навчально - методичне забезпечення	Навчально-методичні комплекси навчальних дисциплін, програми і бази для проходження практик, підручники, словники, навчальні посібники, довідкова література, фахові періодичні видання тощо. Офіційний веб-сайт http://www.zntu.edu.ua містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила

	прийому, контакти. Всі зареєстровані в ЗНТУ користувачі мають необмежений доступ до мережі Інтернет. Матеріали навчально-методичного забезпечення освітньо-професійної програми викладені на освітньому порталі http://www.zntu.edu.ua/kafedra-zahistu-informaciyi. Бібліотечний фонд наукової бібліотеки ЗНТУ на 01.09.2018 р. складають паперові видання у обсязі 895285 примірників навчальної та наукової літератури та електронні видання у обсязі 55717 примірників. У ЗНТУ 8 читальних залів площею 773 $м^2$ на 454 посадкових місця. Комп'ютерна мережа бібліотеки налічує 2 сервери, 7 сканерів, 7 принтерів, 2 копіювальні апарати, 1 багато-функціональний пристрій та 83 комп'ютера, які об'єднані в єдину інформаційну мережу. Всі ресурси бібліотеки доступні через сайт університету http://zntu.edu.ua/naukova-biblioteka.
9 – Академічна мобільність	
Національна кредитна мобільність	На підставі договорів про співробітництво між Запорізьким національним технічним університетом та вітчизняними вищими навчальними закладами (науковими установами) України.
Міжнародна кредитна мобільність	На підставі міжнародних договорів про співробітництво в галузі освіти та науки, міжнародних програм та проектів, договорів про співробітництво між Запорізьким національним технічним університетом та іноземними вищими навчальними закладами (науковими установами) на основі індивідуальних запрошень та інших механізмів.
Навчання іноземних здобувачів вищої освіти	Навчання іноземних здобувачів вищої освіти проводиться на загальних умовах з додатковою мовною підготовкою.

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

2.1 Перелік компонент ОПП

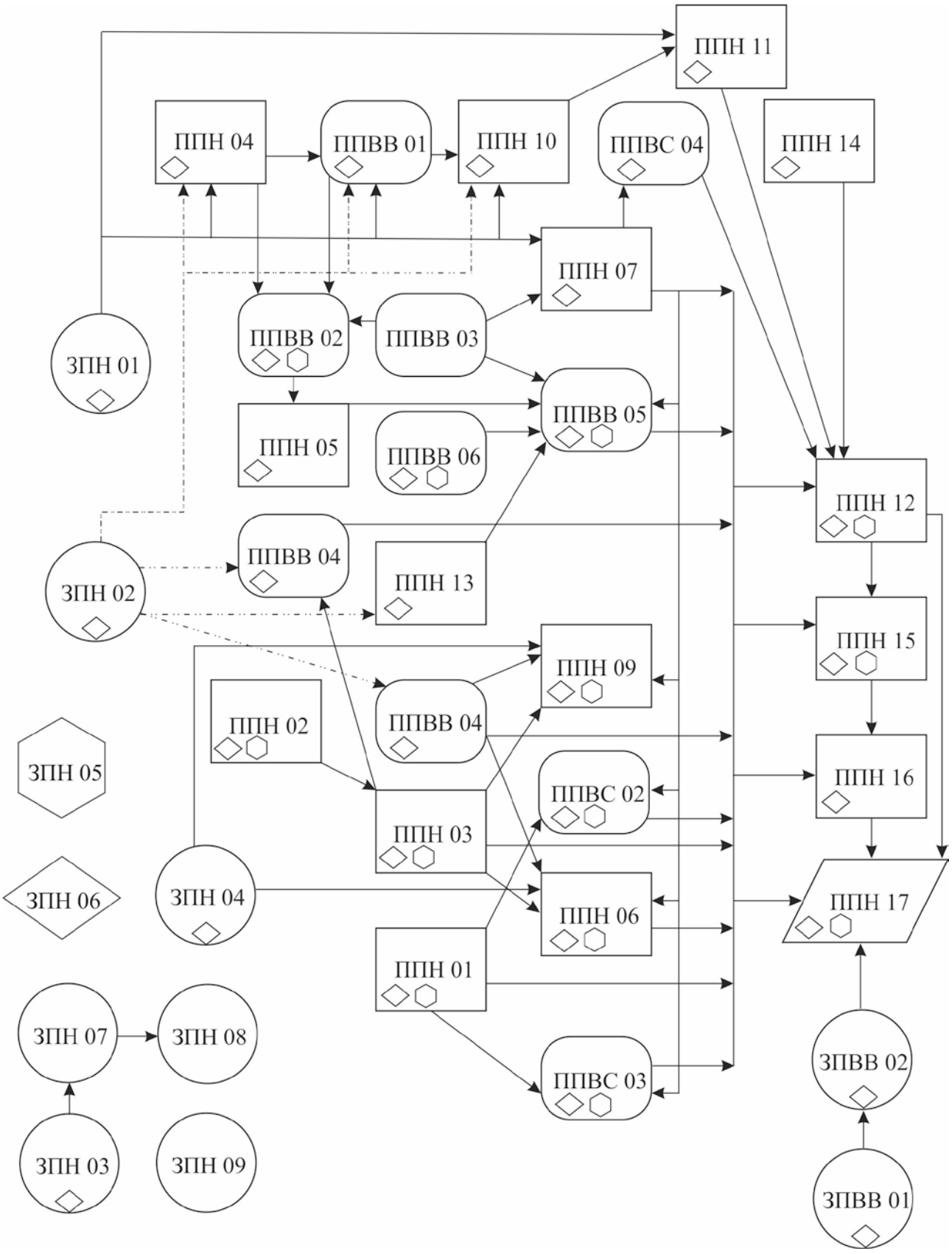
Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
1 ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
1.1	**1.1 НОРМАТИВНА ЧАСТИНА**		
ЗПН 01	Вища математика	18	залік/екзамен
ЗПН 02	Фізика	11	залік/екзамен
ЗПН 03	Історія України	3	екзамен
ЗПН 04	Політико-правова система України	3	залік
ЗПН 05	Іноземна мова	6	залік/екзамен
ЗПН 06	Українська мова (за професійним спрямуванням)	3	екзамен
ЗПН 07	Історія української культури	3	екзамен
ЗПН 08	Філософія	3	екзамен
ЗПН 09	Фізичне виховання	12	залік
1.1	**Всього**	**62**	
1.2	**1.2 ВИБІРКОВА ЧАСТИНА. ЦИКЛ ДИСЦИПЛІН САМОСТІЙНОГО ВИБОРУ ВНЗ**		
ЗПВВ 01	Економічна теорія	3	екзамен
ЗПВВ 02	Економіка за видами діяльності	3	залік
1.2	**Всього**	**6**	
1	**Разом**	**68**	
2	**2 ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ**		
2.1	**2.1 НОРМАТИВНА ЧАСТИНА**		
ППН 01	Технології програмування	11	залік/екзамен/ курсова робота
ППН 02	Інформаційна діяльність та кібербезпека	4	залік
ППН 03	Нормативно-правове і організаційне забезпечення інформаційної безпеки	7	залік/екзамен
ППН 04	Основи теорії кіл, сигналів та процесів в електроніці	9	залік/курсова робота
ППН 05	Телекомунікаційні та комп'ютерні мережі	7	залік/екзамен
ППН 06	Захист інформації в банківській сфері та електронному бізнесі	4	екзамен

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
ППН 07	Основи криптографії та стеганографії	8	залік/екзамен
ППН 08	Методи та засоби технічного захисту інформації	8	залік/курсова робота
ППН 09	Менеджмент інформаційної безпеки	8	залік/екзамен
ППН 10	Схемотехніка пристроїв технічного захисту інформації	8,5	залік/курсовий проект
ППН 11	Технічні засоби охорони об’єктів	8	залік/курсова робота
ППН 12	Проектування, впровадження та супровід комплексних систем захисту інформації	7,5	залік/курсовий проект
ППН 13	Мікрохвильові та оптоелектронні системи передачі	4	екзамен
ППН 14	Безпека життєдіяльності фахівця з основами охорони праці	3	залік
ППН 15	Виробнича практика	9	залік Д
ППН 16	Переддипломна практика	3	залік Д
ППН 17	Дипломування	9	екзамен
2.1	**Всього**	**118**	
2.2	**2.2 ВИБІРКОВА ЧАСТИНА. ЦИКЛ ДИСЦИПЛІН САМОСТІЙНОГО ВИБОРУ ВНЗ**		
ППВВ 01	Основи цифрової електроніки	8	залік/курсова робота
ППВВ 02	Системи передачі інформації	7	залік/екзамен
ППВВ 03	Теорія інформації і кодування	4	екзамен
ППВВ 04	Спеціальні вимірювання в технологіях захисту інформації	4	залік
ППВВ 05	Захищені мережні технології	7	залік/екзамен
ППВВ 06	Цифрові системи обробки сигналів та зображень	7	залік/екзамен
2.2	**Всього**	**37**	
2.3	**2.3 ВИБІРКОВА ЧАСТИНА. ЦИКЛ ДИСЦИПЛІН ВІЛЬНОГО ВИБОРУ СТУДЕНТА**		
ППВС 01	Захищені операційні системи та бази даних / Управління персоналом та кадрова безпека	3	екзамен
ППВС 02	Інтелектуальні системи інформаційної безпеки / Програмно-апаратні засоби захисту інформації	4	залік

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
ППВС 03	Безпека інформаційно-комунікаційних систем /Антивірусні технології	7	залік/екзамен
ППВС 04	Протоколи цифрового підпису / Моделі та методи прийняття рішень	3	залік
2.3	**Всього**	**17**	
2	**Разом**	**172**	
Загальний обсяг нормативних компонент		**180**	
Загальний обсяг вибіркових компонент		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

Позначення та скорочення, наведені в таблиці:
ВНЗ – вищий навчальний заклад;
ЗПН – нормативна дисципліна циклу загальної підготовки;
ЗПВВ – вибіркова дисципліна циклу самостійного вибору ВНЗ;
ППН – нормативна дисципліна циклу професійної підготовки;
ППВВ – вибіркова дисципліна частини циклу самостійного вибору ВНЗ;
ППВС – вибіркова дисципліна циклу вільного вибору студента.

2.2 Структурно-логічна схема ОПП



3. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація випускників освітньо-професійної програми спеціальності 125 «Кібербезпека» проводиться у формі захисту кваліфікаційної роботи та завершується видачею документа встановленого зразка про присудження ступеня бакалавра із присвоєнням кваліфікації: бакалавр із організації захисту інформації з обмеженим доступом.

Атестація здійснюється відкрито та публічно.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

	ЗПН 01	ЗПН 02	ЗПН 03	ЗПН 04	ЗПН 05	ЗПН 06	ЗПН 07	ЗПН 08	ЗПН 09	ЗПВВ 01	ЗПВВ 02	ППН 01	ППН 02	ППН 03	ППН 04	ППН 05	ППН 06	ППН 07	ППН 08	ППН 09	ППН 10	ППН 11	ППН 12	ППН 13	ППН 14	ППН 15	ППН 16	ППН 17	ППВВ 01	ППВВ 02	ППВВ 03	ППВВ 04	ППВВ 05	ППВВ 06	ППВС 01	ППВС 02	ППВС 03	ППВС 04
КЗ 1	•	•			•	•		•		•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
КЗ 2												•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	
КЗ 3	•	•	•	•	•	•				•	•	•	•	•	•		•		•	•	•	•	•	•				•	•	•	•	•	•	•	•	
КЗ 4										•	•	•			•	•	•	•	•			•	•	•	•	•	•	•	•								•
КЗ 5	•	•	•	•	•	•	•	•		•	•	•	•	•	•		•		•	•	•	•	•		•	•	•	•		•	•	•	•	•	•	•	/ •
КЗ 6			•	•				•																												/ •	
КЗ 7			•	•	•	•	•	•	•		•																										
КЗ 8	•	•										•			•			•	•			•	•					•		•				• /			•
КФ 1				•										•			•	•							•	•	•	•								/ •	
КФ 2														•					•			•	•		•	•	•	•				•			/ •		•	
КФ 3												•	•		•	•		•	•			•	•		•	•	•	•		•	•	•	•		/ •	/ •	•	/
КФ 4												•	•						•	•	•	•	•	•	•	•	•	•			•	•	•	•	/ •	/ •	•	
КФ 5											•						•		•			•	•			•		•									/ •	
КФ 6																•		•	•		•	•	•	•	•	•	•	•			•	•	•	•	/ •	/ •	•	/
КФ 7															•	•			•	•		•	•		•	•	•	•	•				•					
КФ 8															•				•			•	•	•	•	•	•	•	•			•			/ •		• /	
КФ 9																	•		•			•	•		•	•	•	•								/ •	/ •
КФ 10																•	•		•			•	•	•	•	•	•	•							/ •		
КФ 11															•	•		•	•			•	•		•	•	•	•									• /
КФ 12																			•		•	•	•		•	•	•	•				•	•		/ •		• /	
КФ 13																•	•		•	•		•	•			•		•					•			/ •	/ •	/ •
КФ 14																			•			•	•	•	•	•	•	•						• /		/ •	
КФ 15																			•			•	•		•	•	•	•						• /		/ •	

5. Матриця забезпечення програних результатів навчання (ПРН) відповідним компонентам освітньо-професійної програми

	ЗПН 01	ЗПН 02	ЗПН 03	ЗПН 04	ЗПН 05	ЗПН 06	ЗПН 07	ЗПН 08	ЗПН 09	ЗПВВ 01	ЗПВВ 02	ППН 01	ППН 02	ППН 03	ППН 04	ППН 05	ППН 06	ППН 07	ППН 08	ППН 09	ППН 10	ППН 11	ППН 12	ППН 13	ППН 14	ППН 15	ППН 16	ППН 17	ППВВ 01	ППВВ 02	ППВВ 03	ППВВ 04	ППВВ 05	ППВВ 06	ППВС 01	ППВС 02	ППВС 03	ППВС 04
ПРН 1	•	•	•	•	•	•				•	•	•	•	•	•			•		•	•	•	•	•					•	•	•	•	•	•	•	•	•	
ПРН 2												•	•	•	•	•	•			•	•	•	•	•	•	•	•	•		•	•	•	•	•	⁄	•	•	
ПРН 3									•																												
ПРН 4	•	•	•	•	•	•	•	•		•	•	•	•	•	•			•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	
ПРН 5												•	•	•				•		•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	⁄	•
ПРН 6			•	•			•	•							•																					⁄	•	
ПРН 7										•	•							•				•	•		•	•	•	•								⁄	•	
ПРН 8	•	•											•		•							•	•		•	•	•	•	•	•		•			•	⁄	•	•
ПРН 9				•										•				•	•	•		•	•		•	•	•	•								⁄	•	•
ПРН 10														•				•		•		•			•	•	•	•										
ПРН 11																						•				•	•	•		•			•					
ПРН 12														•				•				•				•	•	•				•			•		•	
ПРН 13																•						•				•	•	•		•			•					
ПРН 14												•								•	•	•		•	•	•	•	•					•					
ПРН 15												•	•		•			•		•	•	•		•	•	•	•	•	•		•		•		•	⁄	•	•
ПРН 16																	•					•			•	•	•	•										
ПРН 17																•	•		•			•			•	•	•	•					•					
ПРН 18														•		•						•				•	•	•			•		•					
ПРН 19												•								•		•			•	•	•	•			•							
ПРН 20																						•			•	•	•	•					•					
ПРН 21																•			•		•	•		•	•	•	•	•					•			⁄	⁄	•
ПРН 22														•		•	•			•	•	•		•	•	•	•	•			•		•		⁄	•		•
ПРН 23																			•			•			•	•	•	•									⁄	•
ПРН 24																	•		•			•				•	•	•										
ПРН 25																			•			•			•	•	•	•								⁄	•	
ПРН 26														•			•		•			•			•	•	•	•								⁄	•	⁄	•
ПРН 27																						•			•	•	•	•										
ПРН 28															•							•			•	•	•	•					•		•	⁄			
ПРН 29																						•			•	•	•	•										
ПРН 30											•						•					•			•	•	•	•										
ПРН 31												•						•				•			•	•	•	•										•	⁄
ПРН 32																					•	•		•	•	•	•	•					•					
ПРН 33												•								•	•			•	•	•	•	•										
ПРН 34			•	•				•																												⁄	•	
ПРН 35																																				⁄		
ПРН 36																																				⁄		