МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

ІНСТИТУТ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Державна служба спеціального зв'язку
та захисту інформації України
Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
«Київський політехнічний інститут
імені Ігоря Сікорського»
Інв.№ 5764 по ж. 25/21-45
від 18 02 2020

ЗАТВЕРДЖУЮ
Голова Вченої ради
КПІ ім. Ігоря Сікорського
_____ М.З. Згуровський
«17» 05 2019 р.
М.П.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

Безпека державних інформаційних ресурсів

перший (бакалаврський) рівень вищої освіти

за спеціальністю **125 Кібербезпека**

галузі знань **12 Інформаційні технології**

кваліфікація **Бакалавр з кібербезпеки**

Ухвалено на засіданні Вченої ради
університету
від «11» 03. 2019 р., протокол № 3

КПІ ім. Ігоря Сікорського
Київ – 2019

ПЕРЕДМОВА

Розроблено робочою групою:

Голова робочої групи:

Завідувач спеціальної кафедри № 1
Рома Олександр Миколайович, д.т.н., с.н.с.

Члени робочої групи:

Олексійчук Антон Миколайович, д.т.н., доцент
професор спеціальної кафедри № 1

Застело Герман Ігорович, к.т.н., доцент,
доцент спеціальної кафедри № 1

Кулініч Олег Миколайович, к.т.н., доцент,
доцент спеціальної кафедри № 1

Освітньо-професійнапрограма розглянута й ухвалена методичною комісією
ІСЗЗІ КПІ ім. Ігоря Сікорського
протокол № 4 від «01» 03.2019 р.

Голова методичноїкомісії
_____ І.М. Гиренко

ЗМІСТ

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

зі спеціальності 125 Кібербезпека
освітньо-професійна програма Безпека державних інформаційних ресурсів

1 – Загальна інформація	
Повна назва ЗВО та інституту/факультету	Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Інститут спеціального зв'язку та захисту інформації
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь – бакалавр Кваліфікація – Бакалавр з кібербезпеки
Рівень з НРК	НРК України – 6 рівень
Офіційна назва освітньої програми	Безпека державних інформаційних ресурсів
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки і 10,5 місяців (4 н.р.)
Наявність акредитації	Сертифікат про акредитацію серія НД №1192656 від 25 вересня 2017
Передумови	Наявність повної загальної середньої освіти
Мова(и) викладання	Українська
Термін дії освітньої програми	До наступної акредитації
Інтернет-адреса постійного розміщення освітньої програми	http://iszzi.kpi.ua
2 – Мета освітньої програми	
Метою освітньо-професійної програми Безпека державних інформаційних ресурсів є формування професійної компетентності фахівців у галузі інформаційних технологій, що спрямовані на здатність вирішувати типові завдання і проблеми в галузі інформаційних технологій, кібербезпеки та здійснювати професійну діяльність для проектування, розробки, впровадження, супроводу та аудиту захищених інформаційних систем та засобів захисту.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація)	Галузь знань – 12 Інформаційні технології Спеціальність – 125 Кібербезпека
Орієнтація освітньої програми	Освітньо-професійна
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта в галузі інформаційних технологій за спеціальністю Кібербезпека

4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Фахівець здатен виконувати професійну роботу за кодами ДК 003:2010. 3439 Фахівець ізорганізації захисту інформації з обмеженим доступом. Замовником фахівців зі спеціальності 125 Кібербезпека виступає Державна служба спеціального зв'язку та захисту інформації України.
Подальше навчання	Продовження освіти за другим (магістерським) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Лекції, практичні (групові) та семінарські заняття, комп'ютерні практикуми, лабораторні роботи,курсові проекти (роботи), тактико-спеціальні заняття, практики, виконання кваліфікаційної роботи.
Оцінювання	Рейтингова система оцінювання, модульні контрольні роботи, усні та письмові екзамени, заліки, тестування.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки або кібербезпеки що характеризується комплексністю та невизначеністю умов.
Загальні компетентності (КЗ)	
КЗ 1	Здатність застосовувати знання у практичних ситуаціях.
КЗ 2	Знання та розуміння предметної області та розуміння професії.
КЗ 3	Здатність професійно спілкуватися державною та іноземною мовою як усно, так і письмово.
КЗ 4	Вміння виявляти,ставити та вирішувати проблеми за професійним спрямуванням.
КЗ 5	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
Загальні компетентності (ЗКв) вибіркової частини	
КЗв1	Здатність до соціальної і професійної взаємодії, до співробітництва
КЗв2	Здатність гнучко адаптуватися до різних професійних ситуацій, проявляти творчий підхід, ініціативу
КЗв 3	Здатність організовувати свою діяльність, працювати автономно та у команді
КЗв 4	Здатність відповідально приймати рішення з урахуванням соціальних і етичних цінностей та правових норм
КЗв 5	Здатність здійснювати виробничу або прикладну діяльність у міжнародному середовищі
КЗв 6	Здатність усвідомлювати й ураховувати соціокультурні розходження в професійній діяльності

КЗв 7	Здатність підтримувати загальний рівень фізичної активності й здоров'я для ведення активної соціальної й професійної діяльності
КЗв 8	Здатність критично оцінювати й переосмислювати накопичений досвід (власний і чужий), аналізувати свою професійну й соціальну діяльність
КЗв 9	Здатність грамотно будувати комунікацію, виходячи із цілей і ситуації спілкування
КЗв 10	Здатність використовувати у професійній діяльності базові знання у галузі природничих, соціально-гуманітарних та економічних наук
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.
КФ2	Здатність до використання інформаційно-комунікаційних технологій , сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
КФ3	Здатність до використання програмних та програмно апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ4	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.
КФ6	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 и 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.
Фахові компетентності вибіркової частини	
КФв 1	Здатність застосовувати математичний апарат для розв'язання практичних задач.
КФв 2	Здатність експлуатувати та обслуговувати спеціалізоване програмне забезпечення і технічні засоби.
КФв 3	Здатність оцінювати стан та (або) здійснювати заходи з підвищення рівня інформаційної та кібернетичної безпеки
КФв 4	Здатність моделювати роботу досліджуваної системи для вирішення задач кібербезпеки
КФв 5	Здатність аналізувати та контролювати безпечність систем криптографічного та технічного захисту інформації
КФв 6	Здатність застосовувати практичні навички при організації процесу технічного обслуговування, поточного ремонту, тривалого зберігання, розробки експлуатаційної документації.

КФв 7	Здатність приймати участь в інформаційно-психологічному протиборстві на користь інтересам України.
КФв 8	Здатність організовувати метрологічне забезпечення апаратних засобів спеціальних інформаційно-телекомунікаційних систем
КФв 9	Здатність засвоювати загальні принципи побудови та функціонування засобів та комплексів криптографічного захисту інформації, принципи, їх схемотехнічної реалізації
КФв 10	Здатність організовувати контроль якості виконання робіт із захисту інформації
7 – Програмні результати навчання	
РН 1	Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.
РН 2	Організовувати власну професійну діяльність, обирати оптимальні методи та способирозв'язання складних спеціалізованих задач та практичних проблем у професійної діяльності, оцінювати їхню ефективність.
РН 3	Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
РН 4	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.
РН 5	Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.
РН 6	Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
РН 7	Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки.
РН 8	Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки.
РН 9	Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
РН 10	Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.
РН 11	Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.
РН 12	Розробляти моделі загроз та порушника.
РН 13	Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
РН 14	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
РН 15	Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
РН 16	Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємств) відповідно до вимог нормативно-правових документів.
РН 17	Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектор та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

РН 18	Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН 19	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
РН 20	Забезпечувати функціонування спеціального програмного забезпечення щодо захисту інформації від руйнуючих програмних впливів,руйнуючих кодів в інформаційно-телекомунікаційних системах.
РН 21	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.
РН 22	Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної та/або кібербезпеки.
РН 23	Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
РН 24	Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
РН 25	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 їх захисту.
РН 26	Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу та захисту інформаційних та інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
РН 27	Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
РН 28	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.
РН 29	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.
РН 30	Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
РН 31	Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
РН 32	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
РН 33	Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
РН 34	Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
РН 35	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.

РН 36	Виявляти небезпечні сигнали технічних засобів.
РН 37	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.
РН 38	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
РН 39	Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
РН 40	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.
РН 41	Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
РН 42	Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
РН 43	Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
РН 44	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.
РН 45	Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
РН 46	Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
РН 47	Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
РН 48	Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
РН 49	Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
РН 50	Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
РН 51	Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.
РН 52	Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.
РН 53	Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
РН 54	Усвідомлювати цінності громадського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
Програмні результати навчання вибіркової частини	
РНв 1	Постійно працювати над поглибленням і вдосконаленням особистісного рівня
РНв 2	Бути наполегливим у розв’язанні професійних проблем, усі свої дії доводити до логічного завершення

РНв 3	Бути завжди спрямованим на досягнення позитивного результату в професійній діяльності
РНв 4	Здійснювати математичні перетворення та розрахунки (на основі знань з алгебри, геометрії, теорії ймовірностей та математичної статистики, дискретної математики, теорії диференціальних рівнянь тощо), які необхідні для виконання професійних обов'язків.
РНв 5	Використовувати системне та прикладне програмне забезпечення, технічні засоби захисту інформації, засоби криптографічного захисту інформації.
РНв 6	Обирати та використовувати ефективні методи забезпечення інформаційної та кібернетичної безпеки.
РНв 7	Виявляти недоліки в роботі засобів захисту даних в складі штатного прикладного та системного програмного забезпечення.
РНв 8	Виконувати технічний аудит безпеки інформаційної системи.
РНв 9	Будувати системи протидії технічним розвідкам.
РНв 10	Проводити спеціальні досліджень.
РНв 11	Розгортати засоби електроживлення на місцевості, готувати їх до використання та використовувати за призначенням.
РНв 12	Виконувати процедури зашифрування та розшифрування повідомлень з використанням шифрів простої заміни та гамування.
РНв 13	Проводити розвідку із застосуванням сучасних приладів.
РНв14	Застосовувати шифри до засобів та комплексів криптографічного захисту інформації згідно з їх цільовим призначенням.
РНв15	Здійснювати аналіз виконання вимог керівних документів, щодо забезпечення безпеки інформації в повсякденній службовій діяльності.
РНв16	Забезпечувати вчасне виконання робіт із професійної діяльності.
РНв17	Контролювати якість виконання робіт із професійної діяльності.

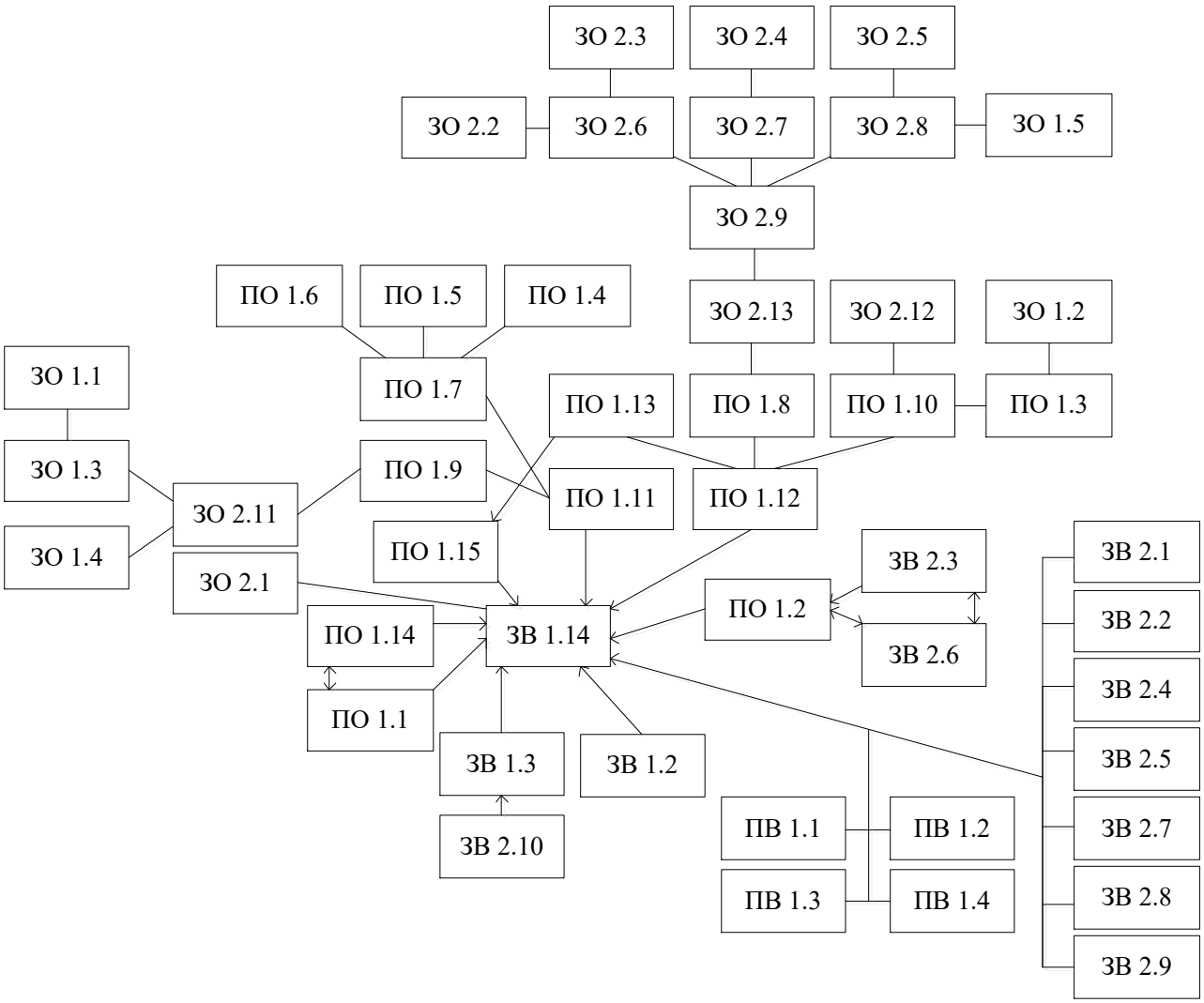
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Відповідно до кадрових вимог щодо забезпечення провадження освітньої діяльності для відповідного рівня ВО затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187(в редакції Постанови КМУ від 10.05.2018 р. №347)
Матеріально-технічне забезпечення	Відповідно до технологічних вимог щодо матеріально-технічного забезпечення освітньої діяльності відповідного рівня ВО (затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187(в редакції Постанови КМУ від 10.05.2018 р. № 347)
Інформаційне та навчально-методичне забезпечення	Відповідно до технологічних вимог щодо навчально-методичного та інформаційного забезпечення освітньої діяльності відповідного рівня ВО затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187(в редакції Постанови КМУ від 10.05.2018 р. № 347)
9 – Академічна мобільність	
Національна кредитна мобільність	Можливість укладання угод про академічну мобільність
Навчання іноземних здобувачів вищої освіти	Можливе навчання іноземних громадян. Навчання іноземних студентів (курсантів) проводиться на загальних умовах або за індивідуальним графіком.

2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬОЇ ПРОГРАМИ

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти/курсові роботи, практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
І. Цикл загальної підготовки			
Обов'язкові компоненти ОП			
1.1. Навчальні дисципліни природничо-наукової підготовки			
ЗО 1.1.	Вища математика	16,5	Екзамен
ЗО 1.2.	Фізика	10	Екзамен
ЗО 1.3.	Теорія ймовірностей і математична статистика	4	Екзамен
ЗО 1.4.	Дискретна математика	7	Екзамен
ЗО 1.5.	Програмування	13,5	Залік
1.2. Навчальні дисципліни базової підготовки			
ЗО 2.1.	Безпека життєдіяльності та цивільний захист	2	Залік
ЗО 2.2.	Архітектура комп'ютерних систем	3	Залік
ЗО 2.3.	Теорія сигналів	4	Екзамен
ЗО 2.4.	Теорія інформації та кодування	3	Екзамен
ЗО 2.5.	Телекомунікаційні та інформаційні мережі	3	Залік
ЗО 2.6.	Комп'ютерні мережі	2	Залік
ЗО 2.7.	Цифрова схемотехніка	2,5	Залік
ЗО 2.8.	Інформаційні технології	2	Залік
ЗО 2.9.	Кібернетична безпека	5	Екзамен
ЗО 2.10.	Економіка і організація виробництва (Організація військового управління)	4	Залік
ЗО 2.11.	Криптографія	4	Залік
ЗО 2.12.	Технічний захист інформації	5	Залік
ЗО 2.13.	Аналіз та моніторинг кібербезпеки	4	Екзамен
Вибіркові компоненти ОП			
1.3. Навчальні дисципліни базової підготовки (за вибором студентів, курсантів)			
ЗВ 1.1.	Технологічна практика	3	Залік
ЗВ 1.2.	Навчальні дисципліни із застосування засобів зв'язку	1,5	Залік
ЗВ 1.3.	Переддипломна практика	3	Залік
ЗВ 1.4.	Дипломне проектування	6	
1.4. Навчальні дисципліни соціально-гуманітарної підготовки (за вибором студентів, курсантів)			
ЗВ 2.1.	Навчальні дисципліни з історії	2	Залік
ЗВ 2.2.	Навчальні дисципліни з української мови	2	Залік
ЗВ 2.3.	Навчальні дисципліни з філософії	2	Залік
ЗВ 2.4.	Навчальні дисципліни з психології	2	Залік
ЗВ 2.5.	Навчальні дисципліни з права	2	Залік
ЗВ 2.6.	Соціально-гуманітарні дисципліни №1	2	Залік
ЗВ 2.7.	Соціально-гуманітарні дисципліни №2	2	Залік
ЗВ 2.8.	Іноземна мова	6	Залік
ЗВ 2.9.	Іноземна мова професійного спрямування	4	Залік
ІІ. Цикл професійної підготовки			

1	2	3	4
Обов'язкові компоненти ОП			
2.1. Навчальні дисципліни обов'язкової професійної та практичної підготовки			
ПО 1.1.	Основи протидії технічним розвідкам	3	Залік
ПО 1.2.	Морально-психологічне забезпечення підрозділів Держспецзв'язку	2	Залік
ПО 1.3.	Технічна електродинаміка	3	Залік
ПО 1.4.	Телекомунікаційні технології	4,5	Екзамен
ПО 1.5.	Теорія електрозв'язку	4	Екзамен
ПО 1.6.	Метрологія та вимірювання	3	Залік
ПО 1.7.	Телекомунікаційні системи	4	Залік
ПО 1.8.	Основи проектування цифрових засобів	4	Залік
ПО 1.9.	Теоретична криптологія	5	Екзамен
ПО 1.10.	Системи та комплекси технічного захисту інформації	4	Екзамен
ПО 1.11.	Засоби та комплекси криптографічного захисту інформації	9	Залік Екзамен
ПО 1.12.	Технології захисту інформації в інформаційно-телекомунікаційних системах	6	Екзамен
ПО 1.13.	Нормативно-правове забезпечення інформаційної безпеки	3	Залік
ПО 1.14.	Основи спеціальних досліджень	5	Екзамен
ПО 1.15.	Безпека спеціального зв'язку	3	Залік
ПО 1.16.	Автомобільна підготовка	2	Залік
ПО 1.17.	Основи організації та забезпечення режиму секретності в установах і організаціях України	1	Залік
ПО 1.18.	Фізичне виховання	17	Залік Екзамен
Вибіркові компоненти ОП			
2.2. Навчальні дисципліни вибіркової професійної та практичної підготовки (за вибором студентів, курсантів)			
ПВ 1.1.	Навчальні дисципліни з тактико-спеціальної підготовки	10	Залік Екзамен
ПВ 1.2.	Навчальні дисципліни з спеціальної (військової) підготовки	11	Залік Екзамен
ПВ 1.3.	Навчальні дисципліни з технічної експлуатації інформаційно-телекомунікаційних систем	3,5	Залік
ПВ 1.4.	Навчальні дисципліни з євроінтеграції	1	Залік
Загальний обсяг **циклузагальноїпідготовки**:		132	
Загальний обсяг **циклупрофесійноїпідготовки**:		108	
Загальний обсяг**обов'язковихкомпонент**:		177	
Загальний обсяг вибіркових компонент (у тому числі за вибором студентів. курсантів)		63	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬОЇ ПРОГРАМИ



4. ФОРМА ВИПУСКНОЇ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Випускна атестація здобувачів вищої освіти за освітньо-професійною програмою “Безпека державних інформаційних ресурсів” здійснюється у формі захисту кваліфікаційної роботи/проекту бакалавра, що забезпечує оцінювання досягнутих програмних результатів навчання, визначених стандартом вищої освіти за спеціальністю 125 “Кібербезпека” для першого (бакалаврського) рівня вищої освіти та освітньо-професійною програмою. Випускна атестація здійснюється відкрито та публічно.

5. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

1. Цикл загальної підготовки

	ЗО 1.1	ЗО 1.2	ЗО 1.3	ЗО 1.4	ЗО 1.5	ЗО 2.1	ЗО 2.2	ЗО 2.3	ЗО 2.4	ЗО 2.5	ЗО 2.6	ЗО 2.7	ЗО 2.8	ЗО 2.9	ЗО 2.10	ЗО 2.11	ЗО 2.12	ЗО 2.13	ЗВ 1.1	ЗВ 1.2	ЗВ 1.3	ЗВ 1.4	ЗВ 2.1	ЗВ 2.2	ЗВ 2.3	ЗВ 2.4	ЗВ 2.5	ЗВ 2.6	ЗВ 2.7	ЗВ 2.8	ЗВ 2.9
КЗ 1		+	+		+		+	+		+	+		+	+			+		+		+										
КЗ2					+		+	+	+			+			+				+	+	+										
КЗ 3																								+						+	+
КЗ 4		+		+		+	+				+	+	+	+			+					+									
КЗ 5			+	+					+	+	+			+		+	+	+				+		+	+						
КЗ 6																							+				+	+			
КЗ 7																								+	+			+			
КЗв1																									+		+				
КЗв 2						+																							+		
КЗв 3																			+												
КЗв 4																								+	+		+				
КЗв 5																+		+					+	+							
КЗв 6																								+	+	+					
КЗв 7						+																									
КЗв 8															+						+			+	+			+			
КЗв 9						+									+										+		+				
КЗв 10	+	+			+		+								+						+										

2. Цикл професійної підготовки

	ПО 1.1	ПО 1.2	ПО 1.3	ПО 1.4	ПО 1.5	ПО 1.6	ПО 1.7	ПО 1.8	ПО 1.9	ПО 1.10	ПО 1.11	ПО 1.12	ПО 1.13	ПО 1.14	ПО 1.15	ПО 1.16	ПО 1.17	ПО 1.18	ПВ 1.1	ПВ 1.2	ПВ 1.3	ПВ 1.4
КФ 1		+											+	+			1					
КФ 2		+		+			+														+	
КФ 3				+				+			+	+		+	+							
КФ 4	+						+							+								
КФ 5					+				+		+				+						+	
КФ 6							+	+											+		+	
КФ 7		+						+		+			+	+								
КФ 8				+											+							
КФ 9		+		+							+					+		+	+			
КФ 10	+								+	+	+	+	+		+							
КФ 11							+							+						+		
КФ 12					+				+			+	+	+							+	
КФв1					+				+													
КФв 2	+										+											
КФв 3												+										
КФв 4	+							+						+								
КФв 5																						
КФв 6			+		+	+				+					+				+			
КФв 7																				+		+
КФв 8			+		+	+												+	+			
КФв 9								+														
КФв 10										+		+			+	+	+		+	+		

6. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

1. Цикл загальної підготовки

	ЗО 1.1	ЗО 1.2	ЗО 1.3	ЗО 1.4	ЗО 1.5	ЗО 2.1	ЗО 2.2	ЗО 2.1	ЗО 2.2	ЗО 2.3	ЗО 2.4	ЗО 2.5	ЗО 2.6	ЗО 2.7	ЗО 2.8	ЗО 2.9	ЗО 2.10	ЗО 2.11	ЗО 2.12	ЗО 2.13	ЗВ 1.1	ЗВ 1.2	ЗВ 1.3	ЗВ 1.4	ЗВ 2.1	ЗВ 2.2	ЗВ 2.3	ЗВ 2.4	ЗВ 2.5	ЗВ 2.6	ЗВ 2.7	ЗВ 2.8	ЗВ 2.9
РН 1																									+	+						+	+
РН 2																											+	+		+			
РН 3		+		+	+				+		+				+	+			+														
РН 4						+	+				+	+				+					+												
РН 5			+		+		+						+	+						+		+		+									
РН 6	+		+						+	+									+				+	+									
РН 7															+		+												+	+			
РН 8															+							+								+			
РН 9																+													+	+			
РН 10	+										+		+		+																		
РН 11							+						+	+						+													
РН 12																			+			+	+										
РН 13					+				+			+				+																	
РН 14									+			+								+				+									
РН 15															+	+				+													
РН 16	+																		+			+	+	+									
РН 17							+						+	+		+																	
РН 18							+						+	+		+																	
РН 19			+	+										+	+			+															
РН 20											+				+																		
РН 21													+	+	+																		
РН 22							+					+	+			+																	

	ЗО 1.1	ЗО 1.2	ЗО 1.3	ЗО 1.4	ЗО 1.5	ЗО 2.1	ЗО 2.2	ЗО 2.1	ЗО 2.2	ЗО 2.3	ЗО 2.4	ЗО 2.5	ЗО 2.6	ЗО 2.7	ЗО 2.8	ЗО 2.9	ЗО 2.10	ЗО 2.11	ЗО 2.12	ЗО 2.13	ЗВ 1.1	ЗВ 1.2	ЗВ 1.3	ЗВ 1.4	ЗВ 2.1	ЗВ 2.2	ЗВ 2.3	ЗВ 2.4	ЗВ 2.5	ЗВ 2.6	ЗВ 2.7	ЗВ 2.8	ЗВ 2.9
РН 23												+		+	+																		
РН 24													+		+	+							+										
РН 25																+				+		+											
РН 26									+			+	+							+													
РН 27							+						+			+				+													
РН28												+		+																			
РН 29																		+	+	+													
РН 30														+	+					+													
РН 31									+					+				+															
РН 32														+	+																		
РН 33															+																		
РН34														+		+																	
РН 35									+		+	+							+														
РН 36										+	+			+					+					+								
РН 37		+																	+			+	+	+								
РН 38				+															+		+		+	+								
РН 39							2							+					+													
РН40							2								+				+													
РН 41												+		+	+																	
РН 42													+		+	+				+	+	+		+								
РН 43													+	+						+												
РН 44				+									+				+			+		+										
РН 45																	+						+									
РН 46																	+						+									
РН 47	+		+	+														+														
РН 48			+									+	+	+																		
РН 49									+				+																			
РН 50			+						+			+		+																		

	ЗО 1.1	ЗО 1.2	ЗО 1.3	ЗО 1.4	ЗО 1.5	ЗО 2.1	ЗО 2.2	ЗО 2.1	ЗО 2.2	ЗО 2.3	ЗО 2.4	ЗО 2.5	ЗО 2.6	ЗО 2.7	ЗО 2.8	ЗО 2.9	ЗО 2.10	ЗО 2.11	ЗО 2.12	ЗО 2.13	ЗВ 1.1	ЗВ 1.2	ЗВ 1.3	ЗВ 1.4	ЗВ 2.1	ЗВ 2.2	ЗВ 2.3	ЗВ 2.4	ЗВ 2.5	ЗВ 2.6	ЗВ 2.7	ЗВ 2.8	ЗВ 2.9
РН 51							+					+				+																
РН 52							+					+	+							+												
РН 53					+															+												
РН 54																											+			+		
РНв 1																	+											+		+		
РНв 2																	+											+			+	
РНв 3																														+	+	
РНв 4	+	+	+	+			+	+	+																							
РНв 5															+			+	+		+		+									
РНв 6													+	+		+																
РНв 7												+	+		+					+	+		+									
РНв 8																				+	+											
РНв 9		+	+							+	+																					
РНв 11		+								+	+			+																		
РНв 12																		+				+										
РНв 13		+					+	+	+					+																		
РНв 14																		+				+										
РНв 15								+	+			+								+												
РНв 16								+	+												+		+									
РНв 17																	+				+		+	+								

2. Цикл професійної підготовки

	ПО 1.1	ПО 1.2	ПО 1.3	ПО 1.4	ПО 1.5	ПО 1.6	ПО 1.7	ПО 1.8	ПО 1.9	ПО 1.10	ПО 1.11	ПО 1.12	ПО 1.13	ПО 1.14	ПО 1.15	ПО 1.16	ПО 1.17	ПО 1.18	ПВ 1.1	ПВ 1.2	ПВ 1.3	ПВ 1.4
РН 1		+																	+	+		
РН 2		+												+		+	+	+	+	+		
РН 3				+							+	+								+		
РН 4		+						+					+	+					+	+		
РН 5		+								+										+	+	
РН 6		+									+						+				+	
РН 7										+	+	+	+									
РН 8												+	+									
РН 9												+	+		+							
РН 10				+	+							+										
РН 11											+	+	+									
РН 12										+		+	+									
РН 13							+	+				+			+						+	
РН 14											+	+	+									
РН 15				+			+	+		+												
РН 16							+			+												
РН 17	+			+				+			+	+							+			
РН 18							+	+		+	+				+							
РН 19				+											+						+	
РН 20											+	+									+	
РН 21				+			+					+									+	
РН 22									+		+			+								
РН 23	+						+		+						+							
РН 24							+					+									+	
РН 25							+	+														

	ПО 1.1	ПО 1.2	ПО 1.3	ПО 1.4	ПО 1.5	ПО 1.6	ПО 1.7	ПО 1.8	ПО 1.9	ПО 1.10	ПО 1.11	ПО 1.12	ПО 1.13	ПО 1.14	ПО 1.15	ПО 1.16	ПО 1.17	ПО 1.18	ПВ 1.1	ПВ 1.2	ПВ 1.3	ПВ 1.4
РН 26				+	+			+	+		+	+										
РН 27				+				+		+	+			+								
РН 28														+	+					+		
РН 29									+			+			+							
РН 30				+						+				+							+	
РН 31								+	+				+									
РН 32				+			+														+	
РН 33				+				+													+	
РН 34													+	+	+							
РН 35										+			+									
РН 36	+									+				+								
РН 37	+		+		+					+				+	+							
РН 38										+			+	+								
РН 39																						
РН 40															+		+					
РН 41								+				+										
РН 42												+									+	
РН 43								+				+	+								+	
РН 44												+	+									
РН 45							+						+									
РН 46								+	+													
РН 47									+				+	+								
РН 48				+				+				+										
РН 49				+				+				+									+	
РН 50							+					+			+						+	
РН 51							+								+						+	
РН 52							+							+								

	ПО 1.1	ПО 1.2	ПО 1.3	ПО 1.4	ПО 1.5	ПО 1.6	ПО 1.7	ПО 1.8	ПО 1.9	ПО 1.10	ПО 1.11	ПО 1.12	ПО 1.13	ПО 1.14	ПО 1.15	ПО 1.16	ПО 1.17	ПО 1.18	ПВ 1.1	ПВ 1.2	ПВ 1.3	ПВ 1.4
РН 53											+			+								
РН 54																						+
РНв 1		+																+		+		
РНв 2																		+		+		
РНв 3		+																		+		
РНв 4			+		+	+			+		+											
РНв 5										+	+	+		+	+							
РНв 6				+								+										
РНв 7													+	+								
РНв 8				+								+		+	+							
РНв 9	+														+							
РНв 10														+	+							
РНв 11	+															+						
РНв12									+		+											
РНв 13	+								+													
РНв 14											+	+	+									
РНв 15													+	+	+		+					
РНв 16		+																	+	+		
РНв 17		+																	+	+		