МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря Сікорського»

ЗАТВЕРДЖУЮ
Голова Вченої ради
КПІ ім. Ігоря Сікорського
_____ Михайло ІЛЬЧЕНКО
«21» 01 2020 р.
М.П.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

Системи, технології та математичні методи кібербезпеки

(Systems, technologies and mathematical methods of cybersecurity)

першого (бакалаврського) рівня

за спеціальністю **125 Кібербезпека**

галузі знань **12 Інформаційні технології**

Кваліфікація **Бакалавр з кібербезпеки**

Ухвалено на засіданні Вченої ради університету від «20» 01 2020 р. протокол № 1

Київ
КПІ ім. Ігоря Сікорського

2020

ПЕРЕДМОВА

Розроблено робочою групою:

Голова робочої групи
Новіков Олексій Миколайович, доктор технічних наук, професор, директор Фізико-технічного інституту

Члени робочої групи:
Архіпов Олександр Євгенович, доктор технічних наук, професор кафедри інформаційної безпеки

Качинський Анатолій Броніславович, доктор технічних наук, професор кафедри інформаційної безпеки

Стьопочкіна Ірина Валеріївна, кандидат технічних наук, доцент кафедри інформаційної безпеки

Прогонов Дмитро Олександрович, кандидат технічних наук, доцент кафедри фізико-технічних засобів захисту інформації

Грайворонський Микола Владленович, кандидат фізико-математичних наук, доцент, **в.о. завідувача кафедри інформаційної безпеки**

Голова групи забезпечення спеціальності

Новіков Олексій Миколайович, доктор технічних наук, професор, директор Фізико-технічного інституту

Гарант освітньої програми

Грайворонський Микола Владленович, кандидат фізико-математичних наук, доцент, **в.о. завідувача кафедри інформаційної безпеки**

Освітня програма розглянута Методичною радою університету
(протокол № 5 від «16» 01 2020 р.)

Голова Методичної ради
_____ Юрій ЯКИМЕНКО

Вчений секретар Методичної ради
_____ Володимир ГОЛОВЕНКІН

До розроблення освітньої програми додатково залучені:

Представники роботодавців:

Мохонько Олексій Анатолійович, кандидат фізико-математичних наук, R&D директор з інформаційної безпеки, ТОВ "Самсунг Електронікс Україна Компані"

Представники студентських організацій:

Мелько Марія, голова Профбюро студентів

Михалко Дмитро, голова Студради ФТІ

Мамчур Ярина, виборний представник студентів

ЗМІСТ

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

зі спеціальності 125 Кібербезпека
за спеціалізацією «Системи, технології та математичні методи кібербезпеки»

1 – Загальна інформація	
Повна ЗВО та інституту/факультету	Національний технічний університет України “Київський політехнічний інститут імені Ігоря Сікорського” Фізико-технічний інститут
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь – бакалавр Кваліфікація – бакалавр з кібербезпеки
Рівень з НРК	НРК України – 8 рівень
Офіційна назва освітньої програми	Системи, технології та математичні методи кібербезпеки
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів, термін навчання 3 роки 10 місяці
Наявність акредитації	Акредитується вперше
Передумови	Наявність повної загальної середньої освіти
Мова(и) викладання	Українська/англійська
Термін дії освітньої програми	До наступної акредитації
Інтернет-адреса постійного розміщення освітньої програми	https://osvita.kpi.ua/node/103
2 – Мета освітньої програми	
1)підготовка фахівців, здатних використовувати і впроваджувати новітні технології та математичні методи і проводити інноваційну діяльність в галузі захисту інформації і кібернетичної безпеки; 2) забезпечення фундаментальної підготовки; 3) гармонійність, багатовимірність освіти; 4) інтеграція науково-інноваційної та практичної діяльності і навчального процесу; 5) орієнтація на міжнародні вимоги в сфері кібербезпеки; 6) орієнтація на вимоги ринку праці та дуальну освіту.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність)	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.
Орієнтація освітньої програми	Освітньо-професійна

Основний фокус освітньої програми та спеціалізації	Базовий фокус ОП – системи та процеси кіберпростору, засоби та заходи захисту. Ключові слова: кібернетична безпека, інформаційно-телекомунікаційні системи, програмні та апаратні засоби захисту інформації, системи і технології кібербезпеки, математичні методи кібербезпеки, аудит кіберінцидентів, технічний аудит
Особливості програми	1) ґрунтовна фундаментальна підготовка у поєднанні із сучасною професійною підготовкою, яка дозволяє проводити інноваційну діяльність і працювати з наукоємними технологіями кібербезпеки; 2) проходження переддипломної практики на базі підприємств-партнерів та участь студентів у виконанні спільних науково-дослідних проектів на замовлення установ та провідних ІТ-компаній України за фахом; 3) підготовка до дуальної освіти в магістратурі.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	3439 “Фахівець із захисту інформації в інформаційних і комунікаційних системах”, “Фахівець із організації інформаційної безпеки” 3121 Фахівець з інформаційних технологій. Освітня кваліфікація - Бакалавр з кібербезпеки Можуть працювати фахівцями із захисту інформації та кібербезпеки в складі відповідних департаментів організацій, підприємств та банків, розробниками та тестувальниками застосунків, що потребують виконання особливих вимог щодо інформаційної та кібернетичної безпеки; співробітниками служб захисту інформації; адміністраторами інформаційної та кібернетичної безпеки, проектувальниками систем захисту в кіберпросторі; розробниками програмних та програмно-апаратних засобів захисту інформації в кіберпросторі, консультантами-інструкторами з кібербезпеки, спеціалістами в галузі кібербезпеки в складі правоохоронних органів, спеціалістами з забезпечення кібербезпеки в кіберпросторі (зокрема, в соціальних мережах; об’єктах з використанням “інтернету речей”, об’єктах критичної інфраструктури (електростанції, водо-, газопостачання тощо)).
Подальше навчання	Продовження освіти за другим (освітньо-професійним, освітньо-науковим) рівнем вищої освіти
5 – Викладання та оцінювання	
Викладання та навчання	Лекції, практичні та семінарські заняття, комп’ютерні практикуми і лабораторні роботи; курсові роботи і індивідуальні завдання; технологія змішаного навчання, практики; виконання дипломної роботи (бакалаврської дипломної роботи)
Оцінювання	На основі рейтингової системи, усних та письмових екзаменів, заліків
6 – Програмні компетентності	
Інтегральна компетентність	Здатність вирішувати складні спеціалізовані задачі та практичні проблеми в області кібернетичної безпеки, що передбачає застосування певних теорій, моделей та методів і характеризується комплексністю та невизначеністю умов.

Загальні компетентності (ЗК)	
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 мовами 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.
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.

Фахові компетентності (ФК)	
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.
КФ 2	Здатність до використання інформаційно- комунікаційних технологій, сучасних методів і моделей інформаційної безпеки.
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 безпеки.
КФ 5	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної безпеки.
КФ 6	Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.
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.)
КФ 8	Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
КФ 9	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою
КФ 10	Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.
КФ 11	Здатність виконувати моніторинг процесів функціонування інформаційних інформаційно- телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/ або кібербезпеки.
КФ 12	Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки
КФ 13	Здатність розв’язувати задачі за фахом із використанням математичних методів, алгоритмів, прикладних та системних програмних рішень та технологій
КФ 14	Здатність розв’язувати задачі із забезпечення конфіденційності, цілісності, доступності та спостережності інформації та керування нею із використанням сучасних технологій, моделей та методів кібербезпеки із врахуванням вимог нормативних документів та стандартів
7 – 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 результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач
ПРН 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
ПРН 5	Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат
ПРН 6	Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності
ПРН 7	Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;
ПРН 8	Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;
ПРН 9	Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки
ПРН 10	Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем
ПРН 11	Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах
ПРН 12	Розробляти моделі загроз та порушника
ПРН 13	Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних
ПРН 14	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень
ПРН 15	Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій
ПРН 16	Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових докПРНентів
ПРН 17	Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; та моделей захисту електронних даних
ПРН 18	Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів
ПРН 19	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах

ПРН 20	Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах
ПРН 21	Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомуні-каційних системах
ПРН 22	Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно- телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;
ПРН 23	Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах
ПРН 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)
ПРН 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 захисту
ПРН 26	Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем
ПРН 27	Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
ПРН 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;
ПРН 29	Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційних та інформаційно-телекомунікаційних системах, ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів
ПРН 30	Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем
ПРН 31	Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем
ПРН 32	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки

ПРН 33	Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;
ПРН 34	Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації
ПРН 35	Вирішувати задачі забезпечення та супроводукомплексних 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 36	Виявляти небезпечні сигнали технічних засобів
ПРН 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;
ПРН 38	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації
ПРН 39	Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах

ПРН 40	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;
ПРН 41	Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур
ПРН 42	Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки
ПРН 43	Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;
ПРН 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;
ПРН 45	Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;
ПРН 46	Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах
ПРН 47	Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;
ПРН 48	Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;
ПРН 49	Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;
ПРН 50	Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення втрогнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);
ПРН 51	Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах
ПРН 52	Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;
ПРН 53	Вирішувати задачі аналізу програмного коду на наявність можливих загроз
ПРН 54	Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні

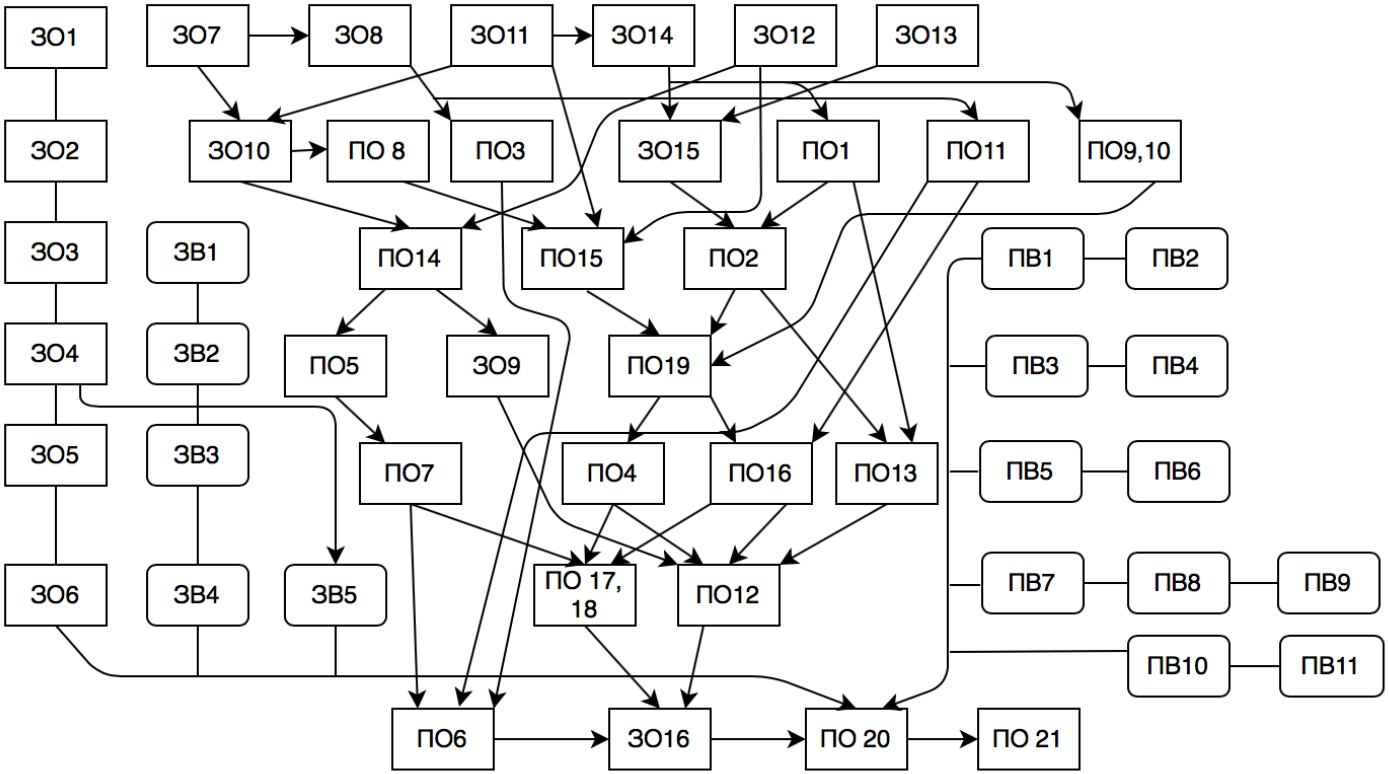
8 – Ресурсне забезпечення реалізації програми	
Кадрове Забезпечення	Відповідно до кадрових вимог щодо забезпечення провадження освітньої діяльності для відповідного рівня ВО (додаток 3 до Ліцензійних умов, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187, за текстом постанови Кабінету Міністрів України від 10.05.2018 р. № 347, п. 28-32)
Матеріально-технічне забезпечення	Відповідно до технологічних вимог щодо матеріально-технічного забезпечення освітньої діяльності відповідного рівня ВО (додаток 4 до Ліцензійних умов, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187, за текстом постанови Кабінету Міністрів України від 10.05.2018 р. № 347, п. 34-35)
Інформаційне та навчально-методичне забезпечення	Відповідно до вимог щодо навчально-методичного та інформаційного забезпечення освітньої діяльності відповідного рівня ВО (додаток 5 до Ліцензійних умов, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187, за текстом постанови Кабінету Міністрів України від 10.05.2018 р. № 347, п.36)
9 – Академічна мобільність	
Національна кредитна мобільність	Участь студентів у програмах академічної мобільності, можливість укладення угод про академічну мобільність
Міжнародна кредитна мобільність	Можливість укладення угод про міжнародну академічну мобільність, про тривалі міжнародні проекти
Навчання іноземних здобувачів вищої освіти	Викладання іноземною мовою (англійською)

2. ПЕРЕЛІК ОБОВ'ЯЗКОВИХ КОМПОНЕНТ 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
1. Нормативні освітні компоненти			
1.1 Цикл загальної підготовки			
ЗО 1	Українська мова за професійним спрямуванням	2	Залік
ЗО 2	Історія науки і техніки	2	Залік
ЗО 3	Фізичне виховання або основи здорового способу життя	5	Залік
ЗО 4	Іноземна мова	6	Залік
ЗО 5	Економіка і організація виробництва	4	Залік
ЗО 6	БЖД та цивільний захист	2	Залік
ЗО 7	Вища математика	17,5	Екзамен
ЗО 8	Фізика	10,5	Залік,Екзамен
ЗО 9	Теорія ймовірностей та математична статистика	5,5	Екзамен
ЗО 10	Дискретна математика	4,5	Екзамен
ЗО 11	Програмування	8,5	Екзамен, Залік
ЗО 12	Алгебра та геометрія	7,5	Екзамен, Залік
ЗО 13	Вступ до кібернетичної безпеки	2	Залік
ЗО 14	Інформаційні технології	3	Залік
ЗО 15	Кібернетична безпека	7	Залік, Екзамен
ЗО 16	Аналіз та моніторинг кібернетичної безпеки	3,5	Екзамен
1. 2 Цикл професійної підготовки			
ПО 1	Архітектура комп'ютерних систем	17,5	Залік
ПО 2	Операційні системи	14,5	Екзамен
ПО 3	Теорія сигналів	5,5	Залік
ПО 4	Комп'ютерні мережі	8,5	Екзамен
ПО 5	Криптографія	13,5	Екзамен
ПО 6	Технічний захист інформації	1	Екзамен
ПО 7	Теорія інформації та кодування	4	Екзамен
ПО 8	Функціональні залежності та структури	5	Екзамен
ПО 9	Основи створення Web-додатків	3	Екзамен
ПО 10	Курсова робота з Основ створення Web-додатків	7	Залік
ПО 11	Оптика	3,5	Залік
ПО 12	Комплексні системи захисту інформації: проектування, впровадження, супровід	3,5	Залік
ПО 13	Системний інжиніринг	1	Залік
ПО 14	Спеціальні розділи математики	6	Екзамен
ПО 15	Алгоритми та структури даних	3	Залік

1	2	3	4
ПО 16	Системи та технології кібернетичної безпеки	3	Екзамен
ПО 17	Безпека операційних систем та комп'ютерних мереж	5	Екзамен
ПО 18	Курсова робота з Безпеки операційних систем та комп'ютерних мереж	5	Залік
ПО 19	Бази даних та інформаційні системи	4	Екзамен
ПО 20	Переддипломна практика	7,5	Залік
ПО 21	Дипломне проектування	2	Захист
2. Вибіркові освітні компоненти			
2.1. Цикл загальної підготовки (Вибіркові освітні компоненти із загальноуніверситетського Каталогу)			
ЗВ 1	Освітній компонент 1 ЗУ-Каталогу	2	Залік
ЗВ 2	Освітній компонент 2 ЗУ-Каталогу	2	Залік
ЗВ 3	Освітній компонент 3 ЗУ-Каталогу	2	Залік
ЗВ 4	Правові Н/Д (Освітній компонент 4 ЗУ-Каталогу)	2	Залік
ЗВ 5	Іноземна мова професійного спрямування	6	Екзамен,Залік
2.2. Цикл професійної підготовки (Вибіркові освітні компоненти з міжфакультетського/факультетського/кафедрального Каталогів)			
ПВ 1	Освітній компонент 1 Ф-Каталогу	4	Залік
ПВ 2	Освітній компонент 2 Ф-Каталогу	4	Залік
ПВ 3	Освітній компонент 3 Ф-Каталогу	4	Залік
ПВ 4	Освітній компонент 4 Ф-Каталогу	4	Залік
ПВ 5	Освітній компонент 5 Ф-Каталогу	4	Залік
ПВ 6	Освітній компонент 6 Ф-Каталогу	4	Залік
ПВ 7	Освітній компонент 7 Ф-Каталогу	4	Залік
ПВ 8	Освітній компонент 8 Ф-Каталогу	4	Екзамен
ПВ 9	Освітній компонент 9 Ф-Каталогу	5	Екзамен
ПВ 10	Освітній компонент 10 Ф-Каталогу	5	Залік
ПВ 11	Освітній компонент 11 Ф-Каталогу	4	Залік
Загальний обсяг циклу загальної підготовки:		**104,5**	
Загальний обсяг циклу професійної підготовки:		**135,5**	
Загальний обсяг нормативних компонент:		**180**	
Загальний обсяг вибіркових компонент по вибору студентів:		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬОЇ ПРОГРАМИ



4. ФОРМА ВИПУСКНОЇ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки» здійснюється у формі публічного захисту кваліфікаційного проекту/роботи. На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання.

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

5. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ НОРМАТИВНИМ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12	КФ13	КФ14
	1	2	3	4	5	6	7	1	2	3	4	5	6	7	8	9	10	11	12	13	14
ЗО1	+	+	+		+				+												
ЗО2	+	+		+	+		+														
ЗО3							+	+													
ЗО4	+	+	+		+				+												
ЗО5					+		+	+											+		
ЗО6						+	+												+		
ЗО7	+	+		+	+				+					+			+		+	+	
ЗО8	+	+	+										+	+			+			+	
ЗО9	+			+					+								+		+	+	
ЗО10	+	+		+					+								+		+	+	
ЗО11	+	+		+	+	+		+	+	+						+		+		+	
ЗО12	+	+		+					+								+		+	+	
ЗО13		+			+																+
ЗО14	+	+	+	+	+				+					+					+	+	
ЗО15	+	+		+					+	+		+		+					+		+
ЗО16	+	+		+	+			+	+	+	+		+	+	+	+	+	+	+		+
ПО1	+	+		+					+	+										+	
ПО2	+	+			+				+									+		+	
ПО3	+	+		+	+				+	+			+				+	+	+		+
ПО4	+	+		+					+	+								+		+	+
ПО5	+	+		+	+			+	+	+			+				+				+
ПО6	+			+					+	+											+
ПО7	+	+		+	+			+	+	+			+				+			+	
ПО8	+	+		+					+								+		+	+	
ПО9	+	+		+	+	+		+	+	+						+		+		+	

ПО10	+	+		+	+	+		+	+	+						+		+		+	
ПО11	+		+		+				+					+		+				+	+
ПО12	+	+		+				+	+		+	+		+					+	+	+
ПО13	+	+		+	+				+	+	+									+	
ПО14	+				+														+	+	
ПО15	+	+	+		+				+					+					+	+	
ПО16	+	+		+	+			+	+	+				+				+	+		+
ПО17	+	+		+	+			+	+	+		+						+	+		+
ПО18	+	+	+	+	+			+	+	+		+							+		+
ПО19	+	+		+	+			+	+	+		+								+	
ПО20	+	+	+	+	+			+	+					+	+	+	+	+	+	+	+
ПО21	+	+	+	+	+			+	+	+	+	+	+	+	+	+	+	+	+	+	+

6. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ НОРМАТИВНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

ПРН	ЗО1	ЗО2	ЗО3	ЗО4	ЗО5	ЗО6	ЗО7	ЗО8	ЗО9	ЗО10	ЗО11	ЗО12	ЗО13	ЗО14	ЗО15	ЗО16	ПО1	ПО2	ПО3	ПО4	ПО5	ПО6	ПО7	ПО8	ПО9	ПО10	ПО11	ПО12	ПО13	ПО14	ПО15	ПО16	ПО17	ПО18	ПО19	ПО20	ПО21
ПРН 1	+	+		+					+	+				+					+							+				+			+			+
ПРН 2		+	+		+		+		+	+	+	+		+		+	+		+		+		+	+	+	+		+	+	+	+				+	+	+
ПРН 3		+					+		+	+	+	+		+			+	+	+		+		+		+	+	+		+	+	+		+	+	+	+	+
ПРН4		+			+		+		+	+		+		+			+		+		+		+	+					+	+	+		+	+	+	+	+
ПРН5		+	+		+		+				+			+											+	+					+					+	+
ПРН6		+			+		+			+		+	+	+	+		+		+		+		+	+			+		+	+	+				+	+	+
ПРН7					+	+					+		+			+					+		+		+	+		+					+	+	+	+	+
ПРН8																					+		+												+	+	+
ПРН9																	+				+		+										+	+	+	+	+
ПРН10							+		+	+	+	+		+	+	+	+	+	+	+	+		+	+	+	+		+	+		+	+	+	+	+	+	+
ПРН11										+	+	+				+								+	+	+		+	+						+	+	+
ПРН12							+	+	+						+	+			+									+				+	+		+	+	+
ПРН13											+				+	+				+					+	+		+	+				+		+	+	+
ПРН14															+	+				+	+	+	+					+				+	+	+	+	+	+
ПРН15											+			+				+							+	+			+		+	+	+	+	+	+	+
ПРН16																+												+								+	+
ПРН17									+																											+	+
ПРН18															+					+		+									+	+			+	+
ПРН19															+	+				+	+		+					+		+				+		+	+
ПРН20																																+		+		+	+
ПРН21																+												+							+	+	+
ПРН22															+						+		+									+	+			+	+
ПРН23																					+	+	+									+				+	+
ПРН24											+				+	+									+	+		+					+	+		+	+
ПРН25																																		+		+	+
ПРН26																																	+	+		+	+
ПРН27																				+	+		+										+	+		+	+
ПРН28									+	+		+				+								+				+						+		+	+

ПРН	ЗО1	ЗО2	ЗО3	ЗО4	ЗО5	ЗО6	ЗО7	ЗО8	ЗО9	ЗО10	ЗО11	ЗО12	ЗО13	ЗО14	ЗО15	ЗО16	ПО1	ПО2	ПО3	ПО4	ПО5	ПО6	ПО7	ПО8	ПО9	ПО10	ПО11	ПО12	ПО13	ПО14	ПО15	ПО16	ПО17	ПО18	ПО19	ПО20	ПО21
ПРН29						+										+												+				+				+	+
ПРН30									+							+						+					+	+								+	+
ПРН31									+						+	+											+	+								+	+
ПРН32									+						+																					+	+
ПРН33						+			+							+												+								+	+
ПРН34																+												+								+	+
ПРН35															+	+					+		+					+								+	+
ПРН36																						+					+									+	+
ПРН37								+														+					+									+	+
ПРН38									+													+					+									+	+
ПРН39																+						+					+									+	+
ПРН40								+	+																		+									+	+
ПРН41																																	+	+		+	+
ПРН42																					+												+	+		+	+
ПРН43																+																				+	+
ПРН44					+											+												+								+	+
ПРН45															+																					+	+
ПРН46																+												+		+						+	+
ПРН47															+						+		+									+			+	+
ПРН48																					+		+									+			+	+
ПРН49																+																		+		+	+
ПРН50																																	+	+		+	+
ПРН51																																	+	+		+	+
ПРН52																+											+							+		+	+
ПРН53																					+		+								+					+	+
ПРН54			+		+	+													+																	+	

Додаток 1

Ф-Каталог для освітньої програми “Системи, технології та математичні методи кібербезпеки” спеціальності 125 Кібербезпека [1]

Назва освітнього компонента	Кре-дити	Семестровий контроль	Силабус
Класичні методи сучасного системного програмування	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Засоби підготовки та аналізу даних	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Теорія скінченних полів	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Моделі рефлексії у кібербезпеці	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Диференціальнірівняння	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Спеціальні розділи програмування	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Методи та технології інформаційно-аналітичних досліджень	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Технології забезпечення якості програмних засобів	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Математичне програмування	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Дослідницький практикум за спеціальністю	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Безпека інтернет-ресурсів	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Моделі та методи прийняття рішень	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Цифрова схемотехніка	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Методи обчислень	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Технології статичного аналізу вихідних кодів	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Системний аналіз	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Технології захисту засобів IoT	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Системи та мережі передачі інформації	4	Екзамен	http://is.ipt.kpi.ua/syllabuses2020
Теорія керування	4	Екзамен	http://is.ipt.kpi.ua/syllabuses2020
Криптографічний захист інформації на мобільних пристроях	4	Екзамен	http://is.ipt.kpi.ua/syllabuses2020
Технічний аудит	5	Екзамен	http://is.ipt.kpi.ua/syllabuses2020
Теорія ризиків	5	Екзамен	http://is.ipt.kpi.ua/syllabuses2020
Безпека мобільних застосунків	5	Екзамен	http://is.ipt.kpi.ua/syllabuses2020
Управління інформаційною безпекою	5	Залік	http://is.ipt.kpi.ua/syllabuses2020

Аналіз даних	5	Залік	http://is.ipt.kpi.ua/syllabuses2020
Основи безпечної розробки програмного забезпечення	5	Залік	http://is.ipt.kpi.ua/syllabuses2020
Нормативно-правове забезпечення інформаційної безпеки	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Нечітке моделювання систем безпеки	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Корпоративні стандарти програмування	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Спеціальні розділи комбінаторного аналізу	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Електроакустичні пристрої	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Гідроакустичні та сейсмоакустичні системи	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Основи метрології	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Вейвлет-аналіз сигналів	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Основи структурного аналізу сигналів	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Автоматизація обробки інформації в технічних системах	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Методи теорії надійності та ризику	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Основи системотехніки	4	Залік	http://is.ipt.kpi.ua/syllabuses2020
Технічні засоби та системи акустичного моніторингу	4	Залік	http://is.ipt.kpi.ua/syllabuses2020

[1] загальнофакультетський Ф-каталог на 2020 рік. Може доповнюватись і оновлюватись щорічно