МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

«ТЕХНІЧНІ СИСТЕМИ КІБЕРЗАХИСТУ»
ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
першого (бакалаврського) рівня вищої освіти
(ПРОЄКТ)

Галузь знань **F «Інформаційні технології»**

Спеціальність **F5 «Кібербезпека та захист інформації»**

Кваліфікація: **«Бакалавр з кібербезпеки та технічного захисту інформації»**

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

Протокол № ____ від _____ 2026 р.

Наказ № ____ від _____ 2026 р.

Ректор _____ Володимир ШУЛЬГА

Освітня програма вводиться в дію з 01 вересня 2026 р.

Київ 2026

ЛИСТ ПОГОДЖЕННЯ
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

спеціальність	F5 «Кібербезпека та захист інформації»
галузь знань	F «Інформаційні технології»
рівень вищої освіти	перший (бакалаврський)
кваліфікація	Бакалавр з кібербезпеки та технічного захисту інформації

1. Перший проректор _____ Олександр КОРЧЕНКО

2. Проректор з навчальної роботи _____ Артур ГУДМАНЯН

3. Начальник навчально-методичного відділу _____ Вадим ВЛАСЕНКО

4. Вчена рада Навчально-наукового інституту кібербезпеки та захисту інформації
Протокол № ____ від «____» _____ 2026 р.

Голова вченої ради ННІКБЗІ _____ Євгенія ІВАНЧЕНКО

Кафедра технічних систем кіберзахисту
Протокол № ____ від «____» _____ 2026 р.

Завідувач кафедри технічних
систем кіберзахисту _____ Олександр ТУРОВСЬКИЙ

Рецензії від зовнішніх стейкхолдерів:

1. ТОВ «ЛУЧ»;
2. ТОВ «А.А.Г.».

ПЕРЕДМОВА

Розроблено робочою групою у складі:

Гарант освітньої програми (голова робочої групи):

Юрій ПЕПА – кандидат технічних наук, доцент, професор кафедри технічних систем кіберзахисту.

Члени робочої групи:

Олександр ТУРОВСЬКИЙ – доктор технічних наук, професор, завідувач кафедри технічних систем кіберзахисту;

Андрій КОТЕНКО – кандидат технічних наук, доцент, доцент кафедри технічних систем кіберзахисту;

Антон ЗАГИНЕЙ – аспірант кафедри технічних систем кіберзахисту.

ВІДОМОСТІ ПРО ПЕРЕГЛЯД ОСВІТНЬОЇ ПРОГРАМИ

Оновлено відповідно до наказу №1547 від 29 жовтня 2024 року «Про внесення змін до стандарту вищої освіти зі спеціальності «Кібербезпека та захист інформації» для першого (бакалаврського) рівня вищої освіти.

Оновлення освітньої програми розроблено відповідно до: наказу Міністерства освіти і науки України від 13.06. 2024 р. № 842; статті 101 Закону України «Про військовий обов'язок і військову службу» (визначено проводити базову загальновійськову підготовку громадян України у закладах вищої освіти всіх форм власності у порядку, визначеному Кабінетом Міністрів України); підпункту 7 пункту 2 розділу II Закону України від 11 квітня 2024 року № 3633- IX «Про внесення змін до деяких законодавчих актів України щодо окремих питань проходження військової служби, мобілізації та військового обліку» (базова загально-військова підготовка, визначена статтею 101 Закону України «Про військовий обов'язок і військову службу», розпочинається з 1 вересня 2025 року); Постанови Кабінету Міністрів України від 21 червня 2024 р. № 734 (затверджено Порядок проведення базової загальновійськової підготовки громадян України, які здобувають вищу освіту, та поліцейських); пропозицій та побажань стейкголдерів (здобувачів вищої освіти, науковопедагогічних працівників, випускників, роботодавців, громадської організації) та з урахуванням тенденцій розвитку спеціальності, ринку праці, галузевого контексту, а також досвіду аналогічних вітчизняних та іноземних освітніх програм. 2026 р. пропозицій та побажань стейкголдерів (здобувачів вищої освіти, науковопедагогічних працівників, випускників, роботодавців, громадської організації) та з урахуванням тенденцій розвитку спеціальності, ринку праці, галузевого контексту, а також досвіду аналогічних вітчизняних та іноземних освітніх програм.

Затверджено рішенням кафедри Технічних систем кіберзахисту,
(назва кафедри)
Протокол № ____ від «___» _____ 2026 р.

Введено в дію наказом ректора № _____ від _____ 2026 року.

1. Профіль освітньої програми

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Державний університет інформаційно-комунікаційних технологій. Навчально-науковий інститут кібербезпеки та захисту інформації.
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр. Освітня кваліфікація – бакалавр з кібербезпеки та захисту інформації.
Офіційна назва освітньої програми	Освітньо-професійна програма «Технічні системи кіберзахисту».
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний на базі повної загальної середньої освіти. Обсяг освітньої програми – 240 кредитів ЄКТС; Термін навчання 3 роки 10 місяців денної форми навчання на базі ступеня молодшого бакалавра (освітньо-кваліфікаційного рівня «молодшого спеціаліста») при перезарахуванні не більше 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки.
Наявність акредитації	Сертифікат про акредитацію спеціальності 125 Кібербезпека УД № 11009229 від 18.04.19 р. Термін дії сертифікату 01.07.2029 р.
Цикл/рівень	НРК України – 6 рівень/Бакалавр QF-EHEA – перший цикл EQF-LLL – 6 рівень
Передумови	Наявність атестата про повну загальну середню освіту або диплома молодшого бакалавра (освітньо-кваліфікаційного рівня «молодший спеціаліст»).
Мова(и) викладання	Українська, англійська.
Термін дії освітньої програми	Програма вводиться в дію з 01.09.2025 року. Програма дійсна впродовж дії державних стандартів вищої освіти та може бути відкоригована відповідно до діючих нормативних документів Університету.
Інтернет-адреса постійного розміщення опису освітньої програми	http://www.duikt.edu.ua/ua/1823-osvitno-profesiyni-programi-kafedra-technicnih-system-kiberzagistu

2 – Мета освітньої програми	
Метою бакалаврської програми є підготовка фахівців здатних використовувати і впроваджувати технічні системи і технології кібербезпеки для захисту інформації, які матимуть здатність розв'язувати складні задачі у галузі кібербезпеки та захисту інформації, з правом подальшої професійної діяльності у державних і комерційних підприємствах та організаціях за спеціальністю.	
3 – Характеристика освітньої програми	
Предметна область, Напрям (галузь знань, спеціальність)	**Об'єкти професійної діяльності випускників:** - об'єкти інформатизації, а саме: комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-комунікаційні системи та мережі, інформаційні ресурси та технології; - системи та технології забезпечення безпеки інформації; - процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. **Теоретичний зміст предметної діяльності.** Знання: - законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; - принципів супроводу систем та комплексів кібербезпеки; - теорії, моделей та принципів управління доступом до інформаційних ресурсів; - методів та засобів виявлення та ідентифікації каналів витоку інформації; - методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; - методів та засобів технічного та криптографічного захисту інформації. F «Інформаційні технології». F5 «Кібербезпека та захист інформації».
Орієнтація освітньої програми	Освітня. 100% обсягу освітньої програми спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю F5 «Кібербезпека та захист інформації» визначеного стандартом вищої освіти. Програма носить прикладний характер, спрямована на забезпечення потреб ринку праці.
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта та професійна підготовка в галузі кібербезпеки та захисту інформації. Підготовка

	фахівців здатних використовувати і впроваджувати технології, методи та засоби інформаційної та кібернетичної безпеки. **Ключові слова:** КІБЕРБЕЗПЕКА, СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ, ВИТІК ІНФОРМАЦІЇ, КІБЕРЗАХИСТ, БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ.
Опис предметної області	**Об'єкти професійної діяльності випускників**: - технології кібербезпеки та захисту інформації; - процеси управління кібербезпекою та захистом інформації; об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології. **Цілі навчання:** підготовка фахівців, здатних використовувати і впроваджувати методи і технології кібербезпеки, а також системи захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації. **Теоретичний зміст предметної діяльності** Принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору та сучасних технологій захисту, які забезпечують сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз інформації, національній безпеці України у кіберпросторі та в інформаційних мережах. **Методи, методики та технології:** методи, методики, технології, способи розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації. **Інструменти та обладнання:** засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси для проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).
Особливості програми	Програма передбачає: - викладання окремих дисциплін циклу професійної підготовки англійською мовою; - передбачено в межах навчального процесу отримання сертифікатів від провідних компаній в галузі інформаційних технологій; - залучення до проведення практичних занять та лабораторних робіт, фахівців-практиків з

	кібербезпеки та захисту інформації; - забезпечення умов підготовки здобувачів вищої освіти у реальному середовищі до майбутньої професійної діяльності для набуття відповідних компетенцій, шляхом організації проведення практик (ознайомча, виробнича та переддипломна) в організаціях-партнерів, з можливістю подальшого працевлаштування.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Бакалавр з кібербезпеки та технічного захисту інформації за освітньою програмою «Технічні системи кіберзахисту» (випускник) здатний виконувати професійні роботи за Державним класифікатором професій ДК 003:2010: - фахівець з технічного захисту інформації; - розробник засобів захисту інформації; - аналітик систем забезпечення кібербезпеки; - проектувальник систем захисту інформації; - провідний спеціаліст/керівник служби ТЗІ та міжнародної стандартної класифікації професій International Standard Classification of Occupation 2008 (ISCO - 08): 2529 Security specialist (ICT). Існує можливість отримати міжнародні сертифікати в галузі кібербезпеки.
Подальше навчання	Можливість продовжити навчання за освітньою програмою другого (магістерського) освітнього рівня вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Проблемно-орієнтоване навчання. Викладання проводиться державною та іноземною (викладання окремих дисциплін проводиться англійською) мовами, які формують професійні компетенції. Викладання спрямовано на засвоєння знань, умінь і навичок для подальшого застосування у практиці. Основними способами передачі змісту освітньої програми є проведення лекцій, семінарських, практичних, індивідуальних, лабораторних занять, консультації, розв’язання ситуаційних задач, тестування, презентації, ознайомча, виробнича, переддипломна практики.
Оцінювання	Оцінювання сформованих компетенцій під час контрольних заходів, які передбачені цією освітньою програмою зазначені у навчальному

	плані. Критерії оцінювання знань, умінь та навичок розроблені у відповідності до чинного законодавства та висвітлено у Положенні про організацію освітнього процесу у Державному університеті інформаційно-комунікаційних технологій.
6 – Програмні компетенції	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області та розуміння професії. ЗК3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК5. Здатність до пошуку, оброблення та аналізу інформації. ЗК6. 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 і Україні. ЗК7. 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.
Спеціальності (фахові предметні компетентності)	СК1. Здатність застосовувати законодавчу та нормативно- правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. СК4. Здатність забезпечувати захист інформації в

	інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. СК5. Здатність відновлювати функціонування Інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. СК6. Здатність впроваджувати та забезпечувати функціонування інформації комплексних (комплекси систем нормативно-правових, захисту організаційних та технічних засобів і методів, процедур, практичних прийомів тощо). СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
7 – Програмні результати навчання	
Результати навчання (РН)	РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

	РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності. РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації. РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних та інформаційно-комунікаційних систем та\або інфраструктури організації в цілому. РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації. РН15. Збирати, обробляти, зберігати, аналізувати

	критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи. РН16. Вирішувати задачі впровадження та супроводу комплексних інформаційних системах. РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації інформаційних системах.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Група забезпечення спеціальності F5 Кібербезпека та захист інформації сформована із числа науково-Педагогічних працівників Навчально-наукового інституту кібербезпеки та захисту інформації. Кількісний та якісний склад групи відповідають ліцензійним вимогам.
Матеріально-технічне забезпечення	Теоретичні заняття проводяться в сучасних комп'ютерних класах та спеціалізованих лабораторіях, які оснащені спеціалізованими апаратно-програмними засобами.

	НАВЧАЛЬНА ЛАБОРАТОРІЯ «Систем технічного захисту інформації на об'єктах інформаційної діяльності». Лабораторія призначена для проведення практичних і лабораторних занять з системами контролю доступом, відеоспостереженням (відеокамери DS-2CD2420F-1, DS-2CD1021-1, DS-2CD4A26FWD-IZS, DS-2CD1331-1, DS-7608NI-E2/8P) і системами раннього реагування на порушення периметру і стороннє втручання (програмно-апаратний комплекс DigiScan EX). НАВЧАЛЬНА ЛАБОРАТОРІЯ «Систем технічного захисту інформації на об'єктах інформаційної діяльності». Лабораторія призначена для вивчення принципів роботи технічних засобів виявлення (пошуковий прилад ST 032) негласних засобів перехоплення інформації (скануючі радіоприймачі AOR-8000, IC-R2500, IC-R20), а також вивчення фізичних принципів роботи систем і блоків засобів захисту інформації (індикатори поля PROTECT 1210, PROTECT 1206i локатор NR-900EM) та блокування витоку інформації (генератор акустичного шуму PIAC-2ГС, генератор електромагнітного радіошуму ST 03.TEST). НАВЧАЛЬНА ЛАБОРАТОРІЯ «Реагування на кіберінциденти». Лабораторія призначена для проведення практичних занять з використанням програмно-апаратних комплексів: IBM QRadar SIEM, IBM i2 Analyze Notebook Premium, Tenable Nessus Professional. Дозволяє відпрацьовувати навички роботи у Центрі забезпечення кібербезпеки (Security Operation Center) з використанням технологій моніторингу, виявлення, аналізу та реагування на кіберінциденти корпоративних інформаційних системах. НАВЧАЛЬНА ЛАБОРАТОРІЯ «Захисту кінцевих точок». Лабораторія використовується для вивчення спеціалізованих засобів криптографічного захисту. Крім того, у лабораторії проводяться тренінги з використанням криптографічних засобів захисту інформації в інформаційно-комунікаційних системах, віртуальних приватних мереж VPN, електронного цифрового підпису та інфраструктури відкритих ключів.

	Спеціалізований програмно-апаратний комплекс ESET Protect дозволяє відпрацьовувати навички для захисту кінцевих точок. НАВЧАЛЬНА ЛАБОРАТОРІЯ «Мережевої безпеки». Лабораторія призначена для вивчення технологій мережевої безпеки CISCO та HUAWEI з можливістю проходження сертифікаційних курсів. НАВЧАЛЬНА ЛАБОРАТОРІЯ «Security Operation Center». Лабораторія призначена для проведення занять з питань аналізу, обробки та аудиту інформаційної безпеки. Крім того, дозволяє вивчати методи управління ризиками на основі методологій CRAMM, OCTAVE та RiskWatch у відповідності до вимог міжнародних стандартів з кібербезпеки та захисту інформації.
Інформаційне та навчально-методичне забезпечення	Інформація про освітню програму, її освітні компоненти та вимоги до осіб, які можуть здобувати вищу освіту за цією програмою розміщена на офіційному сайті Державного університету інформаційно-комунікаційних технологій. Усі освітні компоненти освітньої програми забезпечені навчально-методичними матеріалами, є у вільному доступі у якості ресурсів бібліотеки, системи дистанційного навчання (GWE) університету.
9 – Академічна мобільність	
Національна кредитна мобільність	Наявність двосторонніх договорів між Державним університетом інформаційно-комунікаційних технологій та закладами вищої освіти України забезпечує національну кредитну мобільність.
Міжнародна кредитна мобільність	Зміст навчання відповідає світовим освітнім стандартам, що дозволяє приймати участь у програмах подвійних дипломів та бути конкурентоспроможним на світовому ринку праці.
Навчання іноземних здобувачів вищої освіти	Дозволяє можливість навчання іноземним громадянам.

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

2.1. Зміст підготовки за освітньою програмою, компетентності та результати навчання

№ з.п.	Дисципліна	Шифр	Компетентність	Результат навчання
1. Цикл дисциплін загальної підготовки				
1.	Групова динаміка і комунікації	ЗК12.1.01	ЗК1, ЗК6	ПРН3, ПРН6, ПРН53
2.	Ділові комунікації (Українська мова професійного спрямування)	ЗК12.1.02	ЗК1, ЗК3, ЗК7	ПРН3, ПРН6, ПРН53
3.	Філософія	ЗК12.1.03	ЗК1, ЗК6	ПРН3, ПРН53
4.	Засади відкриття власного бізнесу	ЗК12.1.04	ЗК1, ЗК7	ПРН6, ПРН33, ПРН34
5.	Іноземна мова *	ЗК12.1.05	ЗК3	ПРН1
6.	Вища математика	ЗК12.1.06	ЗК2	ПРН2
7.	Нормативно-правове забезпечення та міжнародні стандарти інформаційної та кібернетичної безпеки	ЗК12.1.07	ЗК2, ЗК3, ЗК5, ПП1	ПРН1, ПРН7, ПРН8, ПРН9, ПРН53
8.	Соціально-екологічна безпека життєдіяльності	ЗК12.1.08	ЗК1 ЗК6, ЗК7	ПРН2
9.	Інформаційно-комунікаційні системи	ЗК12.1.09	ЗК2, ПП2	ПРН2, ПРН5
10.	Фізика	ЗК12.1.10	ЗК2, ЗК7	ПРН2
11.	Теорія інформації та кодування	ЗК12.1.11	ЗК2, ЗК5, ЗК7, ПП2	ПРН2, ПРН36
12.	Менеджмент інформаційної безпеки	ЗК12.1.12	ЗК2, ЗК5, ЗК7, ПП2	ПРН2, ПРН36, ПРН37
2. Цикл дисциплін професійної та практичної підготовки				
1.	Теорія кіл і сигналів в інформаційному та кіберпросторах	ПП12.2.01	ЗК2, ЗК5, ЗК7, ПП2	ПРН2, ПРН36, ПРН37, ПРН38
2.	Прикладне програмування	ПП12.2.02	ЗК2, ЗК5, ПП2	ПРН5, ПРН31, ПРН52
3.	Проектування систем безпеки об’єктів критичної інфраструктури	ПП12.2.03	ЗК2, ПП2	ПРН5, ПРН24, ПРН31
4.	Операційні системи	ПП12.2.04	ЗК1, ПП2	ПРН5, ПРН24, ПРН31, ПРН40

5.	Аналіз та оцінка уразливостей інформаційних систем	ПП12.2.05	ЗК2, ЗК5, ПП2, ПП11	ПРН5, ПРН15, ПРН17, ПРН31
6.	Захист від шкідливого програмного засобу	ПП12.2.06	ЗК1, ЗК3, ЗК5, ПП1	ПРН1, ПРН7, ПРН8
7.	Прикладна криптологія	ПП12.2.07	ЗК2, ЗК7, ПП10	ПРН31, ПРН46, ПРН47
8.	Система менеджменту інформаційної безпеки	ПП12.2.08	ЗК1, ЗК4, ЗК5 ПП5, ПП6, ПП9	ПРН33
9.	Хмарні технології	ПП12.2.09	ЗК2, ЗК5, ПП2, ПП11	ПРН5, ПРН11, ПРН17
10.	Комплексні системи захисту інформації	ПП12.2.10	ЗК1, ЗК4, ЗК5, ПП1, ПП3, ПП7	ПРН5, ПРН7, ПРН15, ПРН16, ПРН21, ПРН27, ПРН29, ПРН35, ПРН39, ПРН43, ПРН48, ПРН50
11.	Системи штучного інтелекту в кібербезпеці	ПП12.2.11	ЗК2, ЗК5, ПП2, ПП11	ПРН5, ПРН17
12.	Компонентна база в системах захисту інформації	ПП12.2.12	ЗК2, ЗК4, ПП5, ПП6, ПП11, ПП12	ПРН12, ПРН14, ПРН15, ПРН36, ПРН37,ПРН38
13.	Поля і хвилі в системах технічного захисту інформації	ПП12.2.13	ЗК2, ЗК5, ПП11	ПРН31, ПРН36, ПРН37,ПРН38
14.	Засоби передачі в системах технічного захисту інформації	ПП12.2.14	ЗК2, ЗК4, ПП3, ПП7, ПП9	ПРН7, ПРН 14, ПРН16, ПРН18, ПРН21, ПРН24, ПРН26, ПРН30, ПРН 50
15.	Засоби прийому та обробки сигналів в системах технічного захисту інформації	ПП12.2.15	ЗК2, ЗК5, ПП8	ПРН4, ПРН12, ПРН19, ПРН23
16.	Методи та засоби технічного захисту інформації	ПП12.2.16	ЗК1, ЗК3, ЗК4, ПП1, ПП4, ПП6, ПП8, ПП9, ПП11, ПП12	ПРН5, ПРН8, ПРН15, ПРН22, ПРН23, ПРН24, ПРН27, ПРН30, ПРН43
17.	Схемотехніка пристроїв технічного захисту інформації	ПП12.2.17	ЗК1, ЗК3, ЗК4, ЗК5, ПП1, ПП2, ПП4, ПП5, ПП6, ПП11, ПП12	ПРН10, ПРН11, ПРН13, ПРН15, 17, ПРН21, ПРН22, ПРН 23, ПРН 25, ПРН 26, ПРН 27, ПРН31, ПРН32
18.	SIEM системи	ПП12.2.18	ЗК2, ЗК3, ЗК4, ПП2, ПП4, ПП5, ПП8, ПП9, ПП11, ПП12	ПРН11, ПРН15, ПРН18, ПРН21, ПРН22, ПРН23, ПРН24, ПРН25, ПРН27, ПРН28, ПРН29, ПРН 40, ПРН43, ПРН48, ПРН 47, ПРН 51
19.	Метрологія та вимірювання в інформаційній безпеці	ПП12.2.19	ЗК2, ЗК5, ПП1, ПП4, ПП5	ПРН4, ПРН19, ПРН22, 28, ПРН44

20.	Технічні засоби охорони об'єктів	ПП12.2.20	ЗК1, ЗК5, ПП1, ПП9	ПРН6, ПРН 15, ПРН 22, ПРН28 ПРН 46, ПРН47
21.	Цифрова криміналістика	ПП12.2.21	ЗК1, ЗК2, ЗК5, ЗК7, ПП1, ПП6, ПП8, ПП10, ПП11, ПП12	ПРН15, ПРН21, ПРН 23, ПРН24, ПРН28, ПРН34, ПРН41, ПРН42, ПРН45
22.	Ознайомча практика	ПП12.2.22	ЗК1, ЗК4	ПРН2, ПРН3, ПРН7
23.	Виробнича практика	ПП12.2.23	ЗК1, ЗК4	ПРН2, ПРН3, ПРН7
24.	Переддипломна практика	ПП12.2.24	ЗК2, ЗК4, ЗК5	ПРН2, ПРН3, ПРН 4, ПРН7
25.	Кваліфікаційна робота	ПП12.2.25	ЗК1, ЗК2, ЗК4, ЗК5, ПП1	ПРН2, ПРН3, ПРН 4, ПРН 6, ПРН7
26.	Підсумкова атестація			
3. Дисципліни вільного вибору студента				
1.	Дисципліна вільного вибору студента			
2.	Дисципліна вільного вибору студента			
3.	Дисципліна вільного вибору студента			
4.	Дисципліна вільного вибору студента			
5.	Дисципліна вільного вибору студента			
6.	Дисципліна вільного вибору студента			
7.	Дисципліна вільного вибору студента			
8.	Дисципліна вільного вибору студента			
9.	Дисципліна вільного вибору студента			

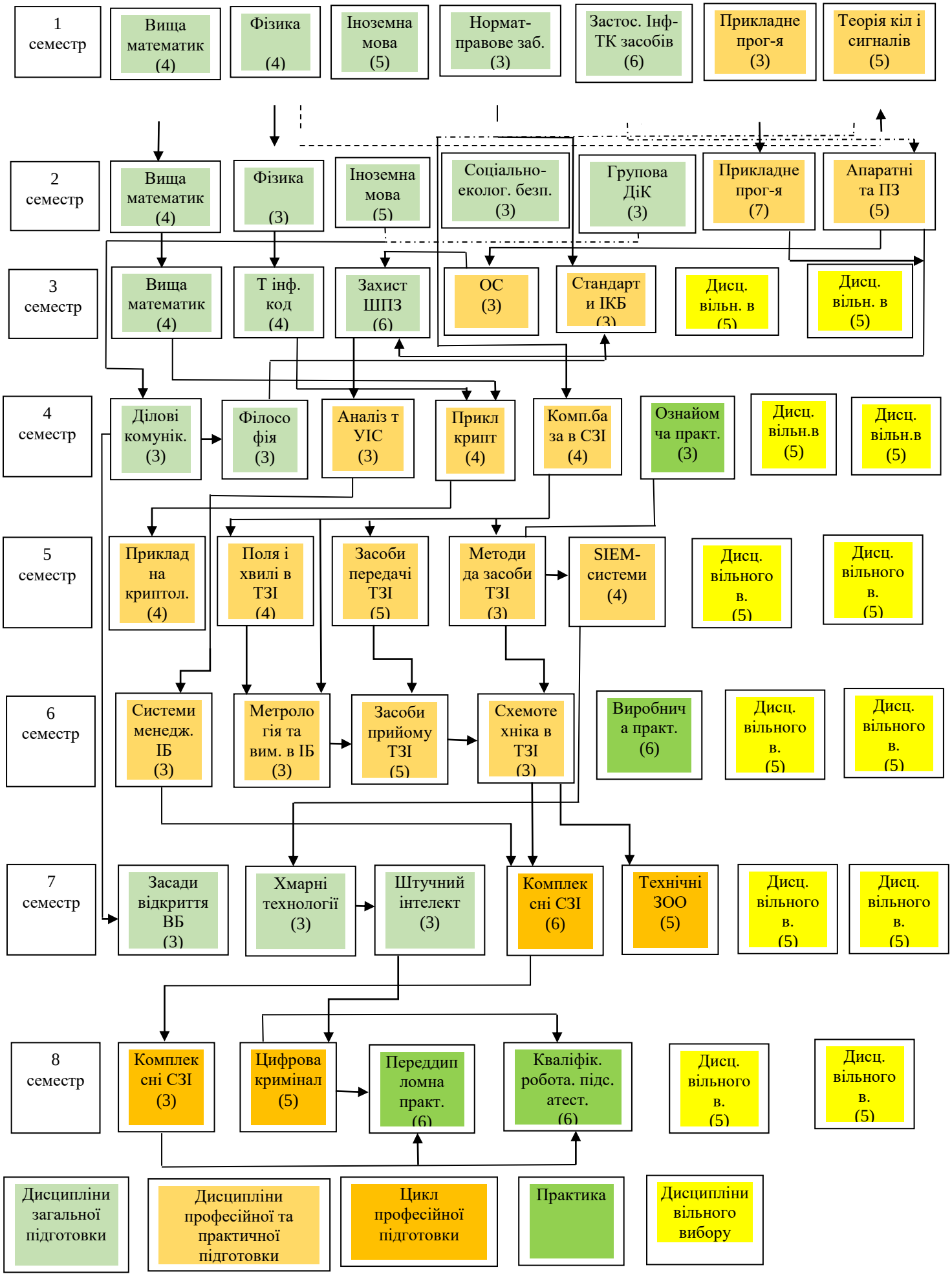
* Іноземна мова у навчальних планах для іноземців та осіб без громадянства замінюється на українську мову (за професійним спрямуванням).

2.2. Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
Обов'язкові компоненти ОП			
ЗК12.1.01	Групова динаміка і комунікації	3	Залік
ЗК12.1.02	Ділові комунікації (Українська мова за професійним спрямуванням)	3	Залік
ЗК12.1.03	Філософія	3	Іспит
ЗК12.1.04	Засади відкриття власного бізнесу	3	Залік
ЗК12.1.05	Іноземна мова	10	Залік, Іспит
ЗК12.1.06	Вища математика	12	Залік, Іспит
ЗК12.1.07	Нормативно-правове забезпечення та міжнародні стандарти інформаційної та кібернетичної безпеки	3	Іспит
ЗК12.1.08	Соціально-екологічна безпека життєдіяльності	3	Іспит
ЗК12.1.09	Інформаційно-комунікаційні системи	6	Залік
ЗК12.1.10	Фізика	7	Залік, Іспит
ЗК12.1.11	Теорія інформації та кодування	4	Іспит
ЗК12.1.12	Менеджмент інформаційної безпеки	3	Іспит
ПП12.2.01	Теорія кіл і сигналів в інформаційному та кіберпросторах	5	Іспит, КР
ПП12.2.02	Прикладне програмування	10	Залік, Іспит
ПП12.2.03	Проектування систем безпеки об'єктів критичної інфраструктури	5	Залік
ПП12.2.04	Операційні системи	3	Іспит
ПП12.2.05	Аналіз та оцінка уразливостей інформаційних систем	3	Іспит
ПП12.2.06	Захист від шкідливого програмного засобу	6	Іспит
ПП12.2.07	Прикладна криптологія	8	Залік, Іспит
ПП12.2.08	Система менеджменту інформаційної безпеки	3	Залік
ПП12.2.09	Мікропроцесорні системи	3	Залік
ПП12.2.10	Комплексні системи захисту інформації	9	Залік, Іспит
ПП12.2.11	Системи штучного інтелекту в кібербезпеці	3	Залік
ПП12.2.12	Компонентна база в системах захисту інформації	4	Іспит
ПП12.2.13	Поля і хвилі в системах технічного захисту інформації	4	Залік, Іспит, КП
ПП12.2.14	Засоби передачі в системах технічного захисту інформації	5	Залік
ПП12.2.15	Засоби прийому та обробки сигналів в системах технічного захисту інформації	5	Залік
ПП12.2.16	Методи та засоби технічного захисту інформації	3	Залік
ПП12.2.17	Схемотехніка пристроїв технічного захисту інформації	3	Іспит
ПП12.2.18	SIEM системи	4	Іспит
ПП12.2.19	Метрологія та вимірювання в інформаційній безпеці	3	Іспит
ПП12.2.20	Технічні засоби охорони об'єктів	5	Іспит
ПП12.2.21	Цифрова криміналістика	5	Іспит

ПП12.2.22	Ознайомча практика	3	Залік
ПП12.2.23	Виробнича практика	6	Залік
ПП11.2.24	Переддипломна практика	6	Залік
ПП11.2.25	Кваліфікаційна робота	5	
	Підсумкова атестація	1	
Загальний обсяг обов'язкових компонент:		**180**	
Вибіркові компоненти ОП			
Дисципліна вільного вибору студента			
Дисципліна вільного вибору студента			
Дисципліна вільного вибору студента			
Дисципліна вільного вибору студента			
Дисципліна вільного вибору студента			
Дисципліна вільного вибору студента			
Дисципліна вільного вибору студента			
Дисципліна вільного вибору студента			
Загальний обсяг вибіркових компонент:		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

2.3. Структурно-логічна схема ОП



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здобувачів вищої освіти здійснюється у формі публічного захисту кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має передбачити розв'язання спеціалізованої задачі в галузі інформаційної та кібербезпеки. Має бути перевірено на плагіат відповідно «Положення про запобігання академічному плагіату у Державному університеті інформаційно-комунікаційних технологій». Оприлюднення на сайті.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ЗК12.1.0 1	ЗК12.1.02	ЗК12.1.03	ЗК12.1.04	ЗК12.1.05	ЗК12.1.06	ЗК12.1.07	ЗК12.1.08	ЗК12.1.09	ЗК12.1.10	ЗК12.1.11	ЗК12.1.12	ППІ2.2.01	ППІ2.2.02	ППІ2.2.03	ППІ2.2.04	ППІ2.2.05	ППІ2.2.06	ППІ2.2.07	ППІ2.2.08	ППІ2.2.09	ППІ2.2.10	ППІ2.2.11	ППІ2.2.12	ППІ2.2.13	ППІ2.2.14	ППІ2.2.15	ППІ2.2.16	ППІ2.2.17	ППІ2.2.18	ППІ2.2.19	ППІ2.2.20	ППІ2.2.21	ППІ2.2.22	ППІ2.2.23	ППІ2.2.24	ППІ2.2.25
1	2	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
ЗК1	+	+	+	+				+				+				+	+			+		+				+	+	+	+		+	+	+	+	+		+
ЗК2						+	+		+	+	+		+	+	+			+	+		+		+	+	+	+	+		+	+	+	+			+	+
ЗК3		+			+		+					+																+		+							
ЗК4																	+			+		+		+		+		+	+	+		+		+	+	+	+
ЗК5							+				+	+	+	+			+				+	+	+		+		+	+	+		+	+			+	+
ЗК6	+		+					+																													
ЗК7		+		+				+		+	+		+						+													+				
ППІ							+					+										+											+				+
ПП2									+		+		+	+	+	+		+			+		+		+	+	+	+		+		+				
ПП3				+																		+					+	+	+			+					
ПП4				+																								+		+							
ПП5				+																+				+		+	+			+		+					
ПП6																+				+				+		+	+	+			+	+	+				
ПП7																						+				+	+	+	+		+	+					
ПП8																	+									+	+	+		+	+	+	+				
ПП9																+				+						+		+		+							
ПП10																	+		+							+	+	+	+		+	+	+				
ПП11																	+				+		+	+		+	+	+		+			+				
ПП12																	+							+		+	+	+		+			+				

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми

	ЗК12.1.01	ЗК12.1.02	ЗК12.1.03	ЗК12.1.04	ЗК12.1.05	ЗК12.1.06	ЗК12.1.07	ЗК12.1.08	ЗК12.1.09	ЗК12.1.10	ЗК12.1.11	ЗК12.1.12	ПП12.2.01	ПП12.2.02	ПП12.2.03	ПП12.2.04	ПП12.2.05	ПП12.2.06	ПП12.2.07	ПП12.2.08	ПП12.2.09	ПП12.2.10	ПП12.2.11	ПП12.2.12	ПП12.2.13	ПП12.2.14	ПП12.2.15	ПП12.2.16	ПП12.2.17	ПП12.2.18	ПП12.2.19	ПП12.2.20	ПП12.2.21	ПП12.2.22	ПП12.2.23	ПП12.2.24	ПП12.2.25
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	22	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38
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																						+		+				+		+	+						

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	29	29	30	31	32	33	34	35	36	37	38
ПРН 28													+				+													+	+	+	+				
ПРН 29													+									+			+		+	+	+	+	+	+					
ПРН 30													+													+	+	+				+					
ПРН 31													+	+	+	+			+						+			+			+						
ПРН 32																									+												
ПРН 33																				+								+				+					
ПРН 34																												+					+				
ПРН 35																						+															
ПРН 36											+		+														+		+		+	+					
ПРН 37													+														+		+		+	+					
ПРН 38													+															+			+	+					
ПРН 39																						+										+					
ПРН 40																+														+							
ПРН 41																											+	+			+		+				
ПРН 42																																	+				
ПРН 43																						+								+							
ПРН 44																																					
ПРН 45																												+			+		+				
ПРН 46																			+							+		+	+								
ПРН 47																			+								+	+		+							
ПРН 48																						+			+		+		+	+	+						
ПРН 49																		+						+													
ПРН 50																						+				+	+	+	+								
ПРН 51																	+	+						+						+	+	+					
ПРН 52														+				+						+													
ПРН 53																																					
ПРН54																																					
ПРН55																																					

Гарант освітньої програми
професор кафедри Технічних систем кіберзахисту, Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій,
кандидат технічних наук, доцент Юрій ПЕПА