МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ОСВІТНЯ ПРОГРАМА
ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА БЕЗПЕКА
першого (бакалаврського) рівня вищої освіти
(оновлена)

Спеціальність **125 Кібербезпека та захист інформації**

Галузь знань **12 Інформаційні технології**

Кваліфікація: **Бакалавр з кібербезпеки та захисту інформації за освітньою програмою інформаційна та кібернетична безпека**

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
Протокол № 10 від 01 квітня 2024 р.
Наказ № 64 від 1 квітня 2024 р.

Ректор _____ Володимир ТОЛУБКО

Освітня програма вводиться в дію з 01 вересня 2024 р.

Київ 2024

ЛИСТ ПОГОДЖЕННЯ
ОСВІТНЬОЇ ПРОГРАМИ
«ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА БЕЗПЕКА»
ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

спеціальність	125 Кібербезпека та захист інформації
галузь знань	12 Інформаційні технології
рівень вищої освіти	перший (бакалавр)
Кваліфікація	бакалавр з кібербезпеки та захисту інформації за освітньою програмою інформаційна та кібернетична безпека

1. Проректор з навчально-виховної роботи _____ Вадим ВЛАСЕНКО
2. Проректор з навчально-виховної та наукової роботи _____ Любов БЕРКМАН
3. Директор Навчально-методичного центру _____ Ірина СРІБНА
4. Вчена рада Навчально-наукового інституту захисту інформації

Протокол № 8 від «18» березня 2024 р.

Голова Вченої Ради ННІЗІ _____ Віталій САВЧЕНКО

5. Кафедра інформаційної та кібернетичної безпеки

Протокол № 8 від «05» березня 2024 р.

Завідувач кафедри інформаційної та кібернетичної безпеки _____ Галина ГАЙДУР

Рецензії від зовнішніх стейкхолдерів:
1. ТОВ «СІТОН ГРУП».
2. Поліський національний університет

ПЕРЕДМОВА

Розроблено робочою групою у складі:

Гарант освітньої програми (голова робочої групи)

Сергій ГАХОВ – кандидат військових наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки

Члени робочої групи:

Галина ГАЙДУР – доктор технічних наук, професор, завідувач кафедри інформаційної та кібернетичної безпеки;

Володимир БОРСУКОВСЬКИЙ – кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки;

Віталій МАРЧЕНКО – доктор філософії, доцент кафедри інформаційної та кібернетичної безпеки;

Сергій ПРИНЬОВ – т.в.о. директора ТОВ «СІТОН ГРУП»;

Анастасія БРИГІНЕЦЬ – студент кафедри інформаційної та кібернетичної безпеки.

ВІДОМОСТІ ПРО ПЕРЕГЛЯД ОСВІТНЬОЇ ПРОГРАМИ

Оновлення (змісту освітніх компонентів та освітньої програми) відповідно до:

Стандарту вищої освіти за спеціальністю 125 Кібербезпека для першого (бакалаврського) рівня вищої освіти

Внесення до Реєстру кваліфікацій відомості щодо професійних стандартів (Наказ Адміністрації Держспецзв'язку від 25 листопада 2022 № 715);

Постанови Кабінету Міністрів України «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 16 грудня 2022 року №1392;

рекомендацій акредитаційних комісій Університету; пропозицій роботодавців; побажань здобувачів вищої освіти.

Внесення до Реєстру кваліфікацій відомості про професійні стандарти у сфері кібербезпеки та захисту інформації від 23 січня 2024 року, рекомендацій стейкхолдерів та побажань здобувачів вищої освіти.

1. Профіль освітньої програми

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Державний університет інформаційно-комунікаційних технологій, Навчально-науковий інститут захисту інформації
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр Освітня кваліфікація – *бакалавр з кібербезпеки та захисту інформації за освітньою програмою інформаційна та кібернетична безпека*
Офіційна назва освітньої програми	Освітня програма «Інформаційна та кібернетична безпека»
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний: на базі повної загальної середньої освіти. Обсяг освітньої програми-240 кредитів ЄКТС; термін навчання 4 роки денної форми навчання та 5 років заочної 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 введена в дію з 01.09.2019 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.dut.edu.ua/ua/1822-osvitno-profesiyni-programi-kafedra-informaciynoi-ta-kibernetichnoi-bezpeki

2 – Мета освітньої програми	
Метою бакалаврської програми є підготовка бакалаврів інформаційної та кібернетичної безпеки з правом подальшої професійної діяльності у державних та комерційних підприємствах та організаціях, формування та розвиток у них загальних і професійних компетентностей в сфері інформаційної та кібернетичної безпеки, що забезпечують здатність випускника виконувати професійну діяльність на первинній посаді, що здатні використовувати і впроваджувати технології інформаційної та кібербезпеки.	
3 – Характеристика освітньої програми	
Предметна область, напрям (галузь знань, спеціальність)	12 Інформаційні технології 125 Кібербезпека та захист інформації
Орієнтація освітньої програми	Освітня. 100% обсягу освітньої програми спрямовано на забезпечення загальних та спеціальних (фахових компетентностей за спеціальністю 125 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 інформаційних технологій. Підготовка фахівців здатних використовувати і впроваджувати технології інформаційної та кібернетичної безпеки. Ключові слова: ІНФОРМАЦІЯ, ЗАГРОЗИ, ВРАЗЛИВОСТІ, ЗАХИЩЕНІСТЬ, КІБЕРБЕЗПЕКА.
Опис предметної області	**Об'єкти професійної діяльності випускників**: об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; технології забезпечення безпеки інформації; процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. **Цілі навчання** підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. **Теоретичний зміст предметної діяльності** Знання: законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; теорії, моделей та

	принципів управління доступом до інформаційних ресурсів; теорії систем управління інформаційною та/або кібербезпекою; методів та засобів виявлення, управління та ідентифікації ризиків; методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; методів та засобів технічного та криптографічного захисту інформації; сучасних інформаційно-комунікаційних технологій; сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; автоматизованих систем проектування. **Методи, методики та технології:** Методи, методики інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки. **Інструменти та обладнання:** системи розробки, забезпечення, моніторингу та контролю інформаційної та/ або кібербезпеки; сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
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, семінарських, практичних занять та лабораторних робіт, фахівців-практиків з інформаційної безпеки; - забезпечення умов підготовки здобувачів вищої освіти у реальному середовищі майбутньої професійної діяльності для набуття відповідних компетенцій, шляхом організації проведення практик (організаційна, виробнича та переддипломна) на фірмах-партнерів, з можливістю подальшого працевлаштування.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Бакалавр з кібербезпеки та захисту інформації за освітньою програмою інформаційна та кібернетична безпека (випускник) здатний виконувати професійні роботи за Державним класифікатором професій ДК 003: 2010: **Основна:** 2139.2 Фахівець з підтримки інфраструктури кіберзахисту Фахівець з реагування на інциденти кібербезпеки

	Молодший адміністратор мереж і систем **Додаткова:** Фахівець з тестування систем захисту інформації Аудитор інформаційних технологій (з кібербезпеки) Фахівець з оцінки заходів захисту інформації (кібербезпеки) Фахівець з криптографічного захисту інформації Фахівець з оцінки заходів захисту інформації (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 та практичні проблеми у галузі забезпечення кібербезпеки та захисту інформації, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (ЗК)	**ЗК1.** Здатність застосовувати знання у практичних ситуаціях. **ЗК2.** Знання та розуміння предметної області та розуміння професії. **ЗК 3.** 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.
Фахові компетенції (КФ)	**КФ1.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та кібербезпеки. **КФ2**. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та 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 кібербезпеки. **КФ5.** Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та 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 і методів, процедур, практичних прийомів та ін.) .

	КФ8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. **КФ9.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та 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 кібербезпеки. **КФ12**. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та кібербезпеки.
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 проблему професійній діяльності, оцінювати їхню ефективність. **ПРН 3.** Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. **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, тому числі міжнародних в галузі інформаційної та

	(в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. **ПРН 22.** Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і 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 згідно встановленої політики інформаційної і кібербезпеки. **ПРН 29.** Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в ІТС та ефективності використання КЗЗ 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 неперервності бізнес процесів організації на основі теорії ризиків. **ПРН 34.** Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та кібербезпеки відповідно до цілей і завдань організації. **ПРН 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 кібербезпеки. **ПРН 36.** Виявляти небезпечні сигнали технічних засобів. **ПРН 37.** Вимірювати параметри небезпечних сигналів для технічних каналів витоку інформації та визначати ефективність захисту від витоку інформації 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.** Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. **ПРН 41.** Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і кібербезпеки. **ПРН 42.** Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та кібербезпеки для розслідування інцидентів. **ПРН 43.** Вирішувати задачі забезпечення неперервності бізнес процесів організації на основі встановленої

	системи управління інформаційною безпекою, згідно вітчизняними та міжнародними вимогами і стандартами. **ПРН 44.** Застосовувати різні класи політик інформаційної безпеки та кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів. **ПРН 45.** Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. **ПРН 46.** Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. **ПРН 47.** Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. **ПРН 48.** Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах. **ПРН 49.** Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). **ПРН 50.** Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах. **ПРН 51.** Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. **ПРН 52.** Вирішувати задачі аналізу програмного коду на наявність можливих вразливостей. **ПРН 53.** Усвідомлювати цінності громадського (вільного демократичного суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина і Україні.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Група забезпечення спеціальності 125 Кібербезпека та захист інформації сформована із числа науково-педагогічних працівників навчально-наукового інституту 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. Для проведення практичних та лабораторних занять з метою формування спеціальних компетентностей зі спеціальності 125 Кібербезпека та захист інформації ОП «Інформаціна та кібернетична безпека» використовуються спеціалізовані лабораторії університету, які оснащені сучасними комп'ютерами та програмно-апаратними комплексами. НАВЧАЛЬНА ЛАБОРАТОРІЯ АКАДЕМІЧНИЙ ЦЕНТР КОМПЕТЕНЦІЙ IBM «КІБЕРПОЛІГОН» Лабораторія призначена для проведення практичних занять з використанням програмно-апаратних комплексів: IBM QRadar SIEM, IBM i2 Analyze Notebook Premium, Tenable Nessus Professional, ESET Protect. Дозволяє відпрацьовувати навички роботи у Центрі забезпечення кібербезпеки (Security Operation Center) з використанням технологій моніторингу, виявлення, аналізу та реагування на кіберінциденти в корпоративних інформаційних системах. НАВЧАЛЬНА ЛАБОРАТОРІЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ НА БАЗІ ТЕХНОЛОГІЙ «АВТОР» Лабораторія використовується для вивчення спеціалізованих засобів криптографічного захисту на базі продуктів компанії АВТОР – партнера кафедри Інформаційної та кібернетичної безпеки. 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. НАВЧАЛЬНА ЛАБОРАТОРІЯ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ CISCO Лабораторія призначена для вивчення технологій мережевої безпеки CISCO та сертифікаційних курсів від партнера кафедри Інформаційної та кібернетичної безпеки – компанії CISCO: Introduction to Cybersecurity, CCNA Security, CCNA Cybersecurity Operations. Лабораторія створена за сприяння компанії CISCO. НАВЧАЛЬНА ЛАБОРАТОРІЯ ЦЕНТР УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРБЕЗПЕКОЮ

	(SECURITY OPERATION CENTER) Лабораторія призначена для проведення занять з питань аналізу, обробки та аудиту інформаційної безпеки за допомогою SIEM-систем та програмних сканерів типу Nessus та Kali Linux. Крім того, дозволяє вивчати методи управління ризиками на основі методологій CRAMM, OCTAVE та RiskWatch у відповідності до вимог міжнародних стандартів з інформаційної та кібербезпеки.
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 (електронної бібліотеки) 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 результатами навчання

№ п.п.	Дисципліна	Шифр	Компетентність	Результат навчання
1. Цикл дисциплін загальної підготовки				
1.	Вища математика	ЗК11.1.01	ЗК2	ПРН2
2.	Основи інформаційної та кібернетичної безпеки	ЗК11.1.02	ЗК2, ПП2,	ПРН2, ПРН5
3.	Фізика	ЗК11.1.03	ЗК2, ЗК7	ПРН2
4.	Нормативно-правове забезпечення інформаційної безпеки	ЗК11.1.04	ЗК2, ЗК3, ЗК5, ПП1,	ПРН1, ПРН7, ПРН8, ПРН9, ПРН 53
5.	Іноземна мова *	ЗК11.1.05	ЗК3	ПРН1
6.	Групова динаміка і комунікації	ЗК11.1.06	ЗК1, ЗК6,	ПРН3, ПРН6, ПРН 53
7.	Соціально-екологічна безпека життєдіяльності	ЗК11.1.07	ЗК1 ЗК6, ЗК7, ПРН 53	ПРН2, ПРН 53
8.	Основи інформаційних технологій	ЗК11.1.08	ЗК2, КФ2,	ПРН5, ПРН15, ПРН31
9.	Основи телекомунікацій	ЗК11.1.09	ЗК1, КФ10	ПРН 5, ПРН10
10.	Теорія інформації та кодування	ЗК11.1.10	ЗК2, ЗК5, ЗК7, ПП2,	ПРН2, ПРН36
11.	Українська мова за професійним спрямуванням	ЗК11.1.11	ЗК1, ЗК3, ЗК7	ПРН3, ПРН6
12.	Філософія	ЗК11.1.12	ЗК1, ЗК6,	ПРН3, ПРН 53
13.	Засади відкриття власного бізнесу	ЗК11.1.13	ЗК1, ЗК7	ПРН6, ПРН33, ПРН34, ПРН 53
2. Цикл дисциплін професійної та практичної підготовки				
1.	Теорія кіл і сигналів в інформаційному та кіберпросторах	ПП11.2.01	ЗК2, ЗК5, ЗК7, ПП2	ПРН2, ПРН36, ПРН37, ПРН38
2.	Прикладне програмування	ПП11.2.02	ЗК2, ЗК5, КФ2,	ПРН5, ПРН31, ПРН52
3.	Стандарти інформаційної та кібербезпеки	ЗК11.1.03	ЗК1, ЗК3, ЗК5, КФ1	ПРН1, ПРН7, ПРН8
4.	Операційні системи	ПП11.2.04	ЗК1, КФ2,	ПРН5, ПРН 15. ПРН31
5.	Захист від шкідливого програмного	ПП11.2.05	ЗК1, ЗК4, КФ5,	ПРН5, ПРН14,

	засобу		КФ6, КФ9	ПРН18, ПРН20, ПРН49, ПРН51, ПРН52
6.	Аналіз та оцінка уразливостей інформаційних систем	ПП11.2.05	ЗК1, ЗК4, ЗК5, КФ8, КФ10, КФ11, КФ12	ПРН3, ПРН9, ПРН18, ПРН28, ПРН51
7.				
8.	Прикладна криптологія	ПП11.2.07	ЗК2, ЗК7, КФ10	ПРН31, ПРН46, ПРН47
9.	Теоретичні основи захищених інформаційно-комунікаційних технологій	ПП11.2.08	ЗК2, ЗК5, КФ2,	ПРН6, ПРН12, ПРН19, ПРН29, ПРН31, ПРН32, ПРН48
10.	SIEM системи	ПП11.2.09	ЗК2, ЗК3, ЗК4, КФ2, КФ4, КФ5, КФ8, КФ9, КФ11, КФ12	ПРН11, ПРН15, ПРН18, ПРН21, ПРН22, ПРН23, ПРН24, ПРН25, ПРН27, ПРН28, ПРН29, ПРН 40, ПРН43, ПРН48, ПРН 47, ПРН 51
11.	Політики безпеки	ПП11.2.10	ЗК2, ЗК5, КФ1, КФ4, КФ5,	ПРН4, ПРН19, ПРН22, 28, ПРН44
12.	Теорія ризиків	ПП11.2.11	ЗК2, ЗК5, КФ8	ПРН4, ПРН12, ПРН19, ПРН23
13.	Програмні комплекси захисту автоматизованих систем від несанкціонованого доступу	ПП11.2.12	ЗК2, ЗК4, КФ3, КФ7, КФ9	ПРН7, ПРН 14, ПРН16, ПРН18, ПРН21, ПРН24, ПРН26, ПРН30, ПРН 50
14.	Система менеджменту інформаційної безпеки	ПП11.2.13	ЗК2, КФ2, КФ 5, КФ 8	ПРН33
15.	Основи захисту конфіденційних даних	КФ11.2.14	ЗК1, ЗК3, ЗК4, КФ1, КФ4, КФ6, КФ8, КФ9, КФ11, КФ12	ПРН5, ПРН8, ПРН15, ПРН22, ПРН23, ПРН24, ПРН27, ПРН30, ПРН43
16.	Основи безпеки комп'ютерних мереж	ПП11.2.15	ЗК1, ЗК3, ЗК4, ЗК5, КФ1, КФ2, КФ4, КФ5, КФ6, КФ11, КФ12	ПРН10, ПРН11, ПРН13, ПРН15, 17, ПРН21, ПРН22, ПРН 23, ПРН 25, ПРН 26, ПРН 27, ПРН31, ПРН32
17.	Безпека Web-ресурсів	ПП11.2.16	ЗК2, ЗК4, КФ5, КФ6, КФ11, КФ12	ПРН12, ПРН14, ПРН15, ПРН21, ПРН23, ПРН25, ПРН27,ПРН49, ПРН51, ПРН52
18.	Комплексні системи захисту інформації	ПП11.2.17	ЗК1, ЗК4, ЗК5, КФ1, КФ3, КФ7	ПРН5, ПРН7, ПРН15, ПРН16, ПРН21, ПРН27,

				ПРН29, ПРН35, ПРН39, ПРН43, ПРН48, ПРН50
19.	Штучний інтелект	ПП11.2.18	ЗК2, ЗК5, КФ2, КФ11	ПРН5, ПРН17
20.	Інфраструктура відкритих ключів	ПП11.2.19	ЗК1, ЗК5, КФ1, КФ9	ПРН6, ПРН 15, ПРН 22, ПРН28 ПРН 46, ПРН47
21.	Основи реагування на інциденти	ПП11.2.21	ЗК2, ЗК4, ЗК5, КФ3, КФ8, КФ9, КФ12	ПРН 2, ПРН 4, ПРН 7, ПРН 12, ПРН 28, ПРН 40, ПРН 41, ПРН 48, ПРН 52
22.	Аудит систем менеджменту інформаційної безпеки	ПП11.2.22	ЗК1, ЗК2, ЗК4, ЗК5, КФ1, КФ9, КФ11, КФ12	ПРН3, ПРН 6, ПРН 7, ПРН15 ПРН 18, ПРН 28, ПРН 29
23.	Цифрова криміналістика	ПП11.2.23	ЗК1, ЗК2, ЗК5, ЗК7, КФ1, КФ6, КФ8, КФ10, КФ11, КФ12	ПРН15, ПРН21, ПРН 23, ПРН24, ПРН28, ПРН34, ПРН41, ПРН42, ПРН45
24.	Ознайомча практика	ПП11.2.24	ЗК1, ЗК4	ПРН2, ПРН3, ПРН7
25.	Виробнича практика	ПП11.2.25	ЗК1, ЗК4	ПРН2, ПРН3, ПРН7
26.	Переддипломна практика	ПП11.2.26	ЗК2, ЗК4, ЗК5,	ПРН2, ПРН3, ПРН 4, ПРН7
27.	Кваліфікаційна робота	ПП11.2.27	ЗК1, ЗК2, ЗК4, ЗК5, КФ1,	ПРН2, ПРН3, ПРН 4, ПРН 6, ПРН7
28.	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			

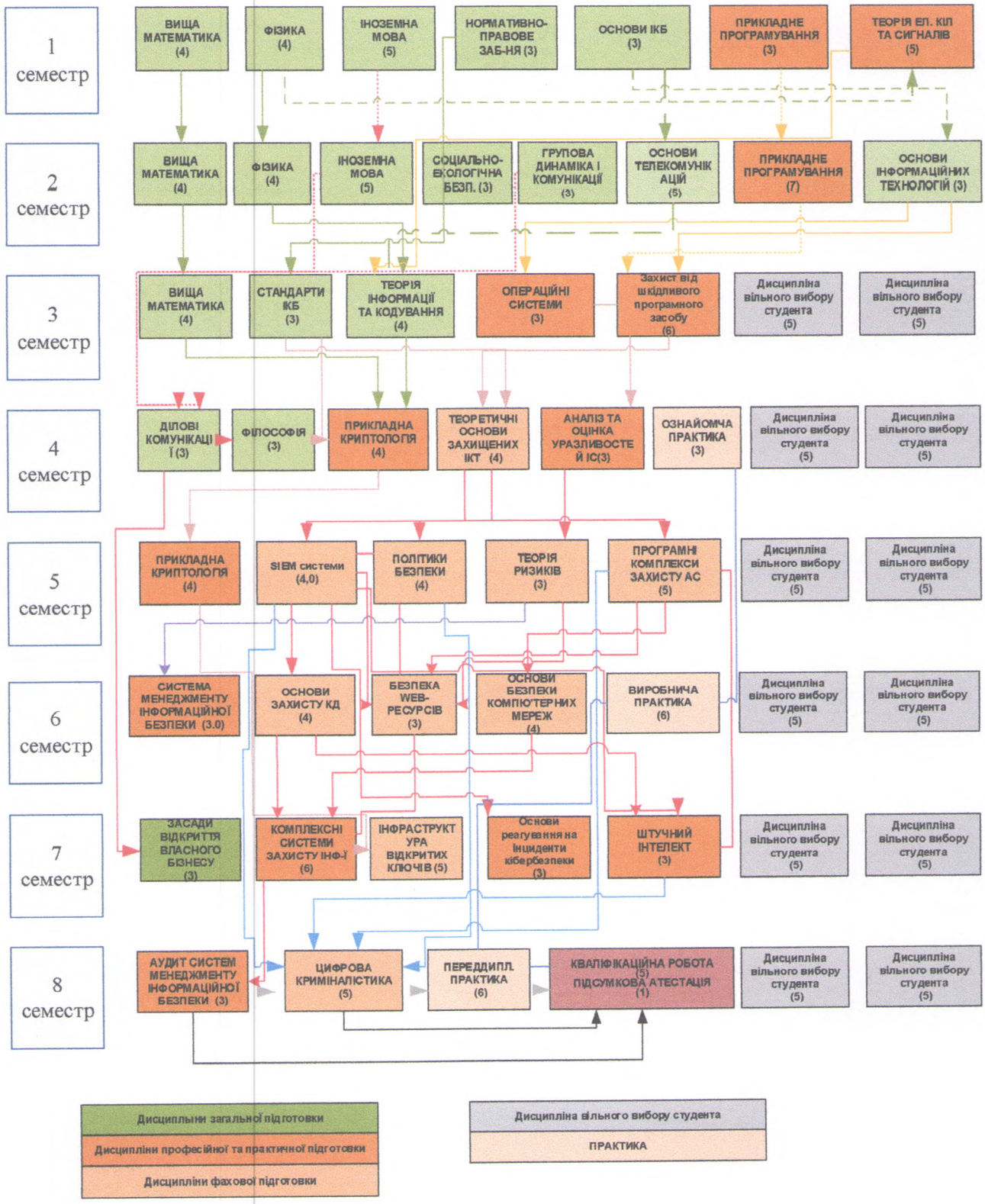
*Іноземна мова у навчальних планах для іноземців та осіб без громадянства замінюється на українську мову (за професійним спрямуванням)

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			
ЗК11.1.01	Вища математика	12	Залік, Іспит
ЗК11.1.02	Основи інформаційної та кібернетичної безпеки	3	Залік
ЗК11.1.03	Фізика	7	Залік, Іспит
ЗК11.104	Нормативно-правове забезпечення інформаційної безпеки	3	Іспит
ЗК11.1.05	Іноземна мова	10	Залік, Іспит
ЗК11.1.06	Групова динаміка і комунікації	4	Залік
ЗК11.1.07	Соціально-екологічна безпека життєдіяльності	3	Іспит
ЗК11.1.08	Основи інформаційних технологій	3	Залік
ЗК11.1.09	Основи телекомунікацій	3	Залік
ЗК11.1.10	Теорія інформації та кодування	4	Іспит
ЗК11.1.11	Українська мова за професійним спрямуванням	3	Залік
ЗК11.1.12	Філософія	3	Іспит
ЗК11.113	Засади відкриття власного бізнесу	3	Залік
ПП11.2.01	Теорія кіл і сигналів в інформаційному та кіберпросторах	5	Іспит
ПП11.2.02	Прикладне програмування	12	Залік, Іспит
ПП11.2.03	Стандарти інформаційної та кібербезпеки	3	Іспит
ПП11.2.04	Операційні системи	3	Залік
ПП11.2.06	Захист від шкідливого програмного засобу	6	Іспит
ПП11.2.05	Аналіз та оцінка уразливостей інформаційних систем	4	Іспит
ПП11.2.07	Прикладна криптологія	8	Залік, Іспит
ПП11.2.08	Теоретичні основи захищених інформаційно-комунікаційних технологій	4	Залік
ПП11.2.09	SIEM системи	4	Іспит
ПП11.2.10	Політики безпеки	3	Іспит
ПП11.2.11	Теорія ризиків	3	Залік
ПП11.2.12	Програмні комплекси захисту автоматизованих систем від несанкціонованого доступу	5	Іспит
ПП11.2.13	Система менеджменту інформаційної безпеки	3	Залік
ПП11.2.14	Основи захисту конфіденційних даних	4	Іспит
ПП11.2.15	Основи безпеки компю'терних мереж	4	Іспит
ПП11.2.16	Безпека Web-ресурсів	3	Іспит
ПП11.2.17	Комплексні системи захисту інформації	6	Іспит
ПП11.2.18	Штучний інтелект	3	Залік
ПП11.2.19	Інфраструктура відкритих ключів	5	Іспит

ПП11.2.20	Основи реагування на інциденти	3	Іспти
ПП11.2.21	Аудит систем менеджменту інформаційної безпеки	3	Іспит
ПП11.2.22	Цифрова криміналістика	5	Іспит
ПП11.2.23	Організаційна практика	3	Залік
ПП11.2.24	Виробнича практика	6	Залік
ПП11.2.25	Переддипломна практика	6	Залік
ПП11.2.26	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			
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 здійснюється у формі єдиного державного кваліфікаційного іспиту та публічного захисту кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має передбачити розв'язання спеціалізованої задачі в галузі кібербезпеки та захисту інформації. Має бути перевірено на плагіат відповідно «Положення про запобігання академічному плагіату у Державному університеті інформаційно-комунікаційних технологій. Кваліфікаційна робота має бути оприлюднена у репозитарії Державного університету інформаційно-комунікаційних технологій.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ЗК11.1.01	ЗК11.1.02	ЗК11.1.03	ЗК11.1.04	ЗК11.1.05	ЗК11.1.06	ЗК11.1.07	ЗК11.1.08	ЗК11.1.09	ЗК11.1.10	ЗК11.1.11	ЗК11.1.12	ЗК11.1.13	ПП11.2.01	ПП11.2.02	ПП.11.2.03	ПП.11.2.04	ПП.11.2.05	ПП.11.2.06	ПП.11.2.07	ПП.11.2.08	ПП.11.2.09	ПП.11.2.10	ПП.11.2.11	ПП.11.2.12	ПП.11.2.13	ПП.11.2.14	ПП.11.2.15	ПП.11.2.16	ПП.11.2.17	ПП.11.2.18	ПП.11.2.19	ПП.11.2.20	ПП.11.2.21	ПП.11.2.22	ПП.11.2.23	ПП.11.2.24	ПП.11.2.25	ПП.11.2.26
ЗК 1						•	•		•							•			•								•	•					•					
ЗК 2	•	•	•	•				•		•				•	•					•	•	•	•	•	•			•		•		•	•			•	
ЗК 3				•	•						•					•						•				•	•	•										
ЗК 4																		•	•			•				•	•	•	•	•			•	•	•	•		
ЗК 5				•						•				•	•	•			•		•		•	•				•		•		•	•	•	•			
ЗК 6						•	•					•																										
ЗК 7			•				•			•	•		•	•						•														•				
КФ1				•												•							•				•	•		•		•		•				•
КФ2		•						•		•				•	•		•				•	•				•			•		•							
КФ3																									•				•			•						
КФ4																						•	•				•	•										
КФ5																		•				•	•			•		•	•									
КФ6																		•									•	•	•						•			
КФ7																								•						•								
КФ8																			•			•		•		•	•						•		•			
КФ9																		•				•			•		•				•		•	•				
КФ10									•										•	•																		
КФ11																			•			•					•	•	•		•			•	•			
КФ12																			•			•					•	•	•				•	•	•			

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

	ЗКІІ.1.01	ЗКІІ.1.02	ЗКІІ.1.03	ЗКІІ.1.04	ЗКІІ.1.05	ЗКІІ.1.06	ЗКІІ.1.07	ЗКІІ.1.08	ЗКІІ.1.09	ЗКІІ.1.10	ЗКІІ.1.11	ЗКІІ.1.12	ЗКІІ.1.13	ІПІІ1.2.01	ІПІІ1.2.02	ІПІ.11.2.03	ІПІ.11.2.04	ІПІ.11.2.05	ІПІ.11.2.06	ІПІ.11.2.07	ІПІ.11.2.08	ІПІ.11.2.09	ІПІ.11.2.10	ІПІ.11.2.11	ІПІ.11.2.12	ІПІ.11.2.13	ІПІ.11.2.14	ІПІ.11.2.15	ІПІ.11.2.16	ІПІ.11.2.17	ІПІ.11.2.18	ІПІ.11.2.19	ІПІ.11.2.20	ІПІ.11.2.21	ІПІ.11.2.22	ІПІ.11.2.23	ІПІ.11.2.24	ІПІ.11.2.25	ІПІ.11.2.26
ПРН1				•	•											•																					
ПРН2	•	•	•				•			•				•																		•		•	•	•	•	
ПРН3						•					•	•							•																•	•	•	•	
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																			•			•	•									•	•	•					
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				•		•	•						•	•																									

Гарант освітньої програми
Доцент кафедри інформаційної та кібернетичної безпеки
Навчально-наукового інституту захисту інформації
Державного університету інформаційно-комунікаційних технологій

Кандидат військових наук, доцент **Сергій ГАХОВ**