МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «ТЕХНІЧНІ СИСТЕМИ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ»

першого (бакалаврського) рівня вищої освіти

Галузь знань 12 «Інформаційні технології»
Спеціальність 125 «Кібербезпека»
Освітня кваліфікація: «Бакалавр з кібербезпеки»
Професійна кваліфікація: 3439 Фахівець із організації захисту інформації з обмеженим доступом

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
Голова вченої ради

Протокол № 11 від 24 березня 2016 р.

Освітня програма вводиться в дію з 01.09.2016 р.

Ректор Голубко В.Б. /_____/

Наказ № 147 від 05 квітня 2016 р.

Київ
2016

ЛИСТ ПОГОДЖЕННЯ
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«ТЕХНІЧНІ СИСТЕМИ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ»
ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

галузь знань	*12 «Інформаційні технології»*
спеціальність	*125 «Кібербезпека»*
рівень вищої освіти	*перший (бакалавр)*
освітня кваліфікація	*Бакалавр з кібербезпеки*
професійна кваліфікація	*3439 Фахівець із організації захисту інформації з обмеженим доступом*

ЛИСТ ПОГОДЖЕННЯ
Освітньо-професійної програми

1. Науково-методична рада протокол № 6 від «22» березня 2016 року

Голова науково-методичної ради _____ В.Б. Толубко

2. Навчально-науковий центр

Директор навчально-наукового центру _____ А.М. Явтушенко

3. Вчена рада Навчально-наукового інституту захисту інформації
протокол № 8 від «11» березня 2016 року

Голова вченої ради інституту _____ В.Л.Шевченко

4. Кафедра систем захисту інформації
протокол № 11 від "4" 03 2016 року

Завідувач кафедри _____ С.В. Лазаренко

5. Рецензії від зовнішніх – стейкхолдерів (фірм-партнерів):

1. Навчально-науково-виробничий комплекс «Інформаційно-комунікаційні системи».

2. Державне підприємство «Український науково-технічний і впроваджувальний центр комплексного захисту інформації» (Український центр «Безпека»).

продовження

ЛИСТ ПОГОДЖЕННЯ
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«ТЕХНІЧНІ СИСТЕМИ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ»
ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

галузь знань *12 «Інформаційні технології»*
спеціальність *125 «Кібербезпека»*
рівень вищої освіти *перший (бакалавр)*
освітня кваліфікація *Бакалавр з кібернетичної безпеки*
професійна кваліфікація *3439 Фахівець із організації захисту інформації з обмеженим доступом*

6. Представник професійної асоціації (ринку праці)

Директор Навчально-наукового-виробничого комплексу «Інформаційно-комунікаційні системи» _____ А.К. Фєнєнков

7. Представник професійної асоціації (ринку праці)

Заступник директора з технічних питань ДП Український центр «Безпека» _____ К.В. Кордонець

«ПОГОДЖЕНО»

Директор Навчально-наукового-виробничого комплексу «Інформаційно-комунікаційні системи»

_____ А.К. Фєнєнков

«ПОГОДЖЕНО»

Заступник директора з технічних питань ДП Український центр «Безпека»

_____ К.В. Кордонець

ПЕРЕДМОВА

Розроблено проектною групою Навчально-наукового інституту захисту інформації Державного університету телекомунікацій у складі:

Керівник:

Труш Олександр Вікторович – доцент кафедри систем захисту інформації, кандидат технічних наук з спеціальності 172 Телекомунікації та радіотехніка (05.12.20 - оптоелектронні системи).

Члени проектної групи:

Єрмошин Валерій Віталійович – доцент кафедри систем технічного захисту інформації Навчально-наукового інституту захисту інформації, кандидат технічних наук з спеціальності 125 Кібербезпека (05.13.21-системи технічного захисту інформації);

Чичикало Ніна Іванівна – професор кафедри електроннної техніки, доктор технічних наук з спеціальності 152 Метрологія та інформаційно-вимірювальна техніка (05.11.16 - інформаційно-вимірювальні системи).

1. Профіль освітньої програми

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Державний університет телекомунікацій, Навчально-науковий інститут захисту інформації
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр Освітня кваліфікація – Бакалавр з кібербезпеки
Офіційна назва освітньої програми	Освітньо-професійна програма «Технічні системи інформаційного та кібернетичного захисту»
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, термін навчання 4 роки - обсяг освітньої програми: на базі повної загальної середньої освіти - 240 кредитів ЄКТС; на базі ступеня «молодший бакалавр» (освітньо- кваліфікаційного рівня «молодший спеціаліст») – 180 кредитів ЄКТС.
Наявність акредитації	Розробляється вперше
Цикл/рівень	НРК України – 6 рівень/ Бакалавр, QF-EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Наявність атестата про повну загальну середню освіту
Мова(и) викладання	Українська, англійська
Термін дії освітньої програми	Ввведена в дію з 01.09.2016 року
Інтернет - адреса постійного розміщення опису освітньої програми	http://www.dut.edu.ua/ua/1823-osvitno-profesiyni-programi-kafedra-sistem-informaciynogo-ta-kibernetichnogo-zahistu
2 – Мета освітньої програми	
Метою бакалаврської програми є підготовка фахівців із організації захисту інформації з обмеженим доступом з правом подальшої професійної діяльності у державних та комерційних підприємствах та організаціях, формування та розвиток у них загальних і професійних компетентностей у сфері інформаційної та кібербезпеки, що забезпечують здатність випускника виконувати професійну діяльність на первинній посаді, пов'язаній з технічним захистом інформації.	

3 – Характеристика освітньої програми	
Предметна область, напрям (галузь знань, спеціальність)	12 Інформаційні технології 125 Кібербезпека
Орієнтація освітньої програми	Освітньо-професійна. Програма носить прикладний характер, спрямована на забезпечення потреб ринку праці, зокрема у сфері кібербезпеки.
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта та професійна підготовка галузі інформаційних технологій. Підготовка фахівців для роботи у сфері технічного захисту інформації на підприємствах в установах та організаціях. Ключові слова: ІНФОРМАЦІЯ, ЗАГРОЗИ, ВРАЗЛИВОСТІ, ЗАХИЩЕНІСТЬ, КІБЕРБЕЗПЕКА, ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ.
Особливості програми	Програма передбачає викладання навчальних дисциплін спеціалістами у сфері інформаційної та кібербезпеки, технічного захисту інформації, що суттєво поглиблює фахові компетентності майбутніх випускників. Передбачено проведення лекційних курсів, семінарських та практичних занять, лабораторних робіт, з залученням фахівців із захисту інформації.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Бакалавр з кібербезпеки (випускник) здатний виконувати професійні роботи за Державним класифікатором професій ДК 003: 2010: **Основна:** *3439 Фахівець із організації захисту інформації з обмеженим доступом* Додаткова: *3439* Фахівець з організації інформаційної безпеки *3121* “Фахівець з інформаційних технологій” *3114* Фахівець інфокомунікацій *3119 Технік* (сфера захисту інформації)
Подальше навчання	Продовжити освіту за другим освітнім рівнем вищої освіти
5 – Викладання та оцінювання	
Викладання та навчання	Проблемно-орієнтоване навчання, яке доповнюється практичними складовими компаніями партнерами
Оцінювання	Письмові та усні екзамени, тестування знань, усні презентації, поточний контроль, звіти про практику, захист бакалаврської роботи.

6- Програмні компетенції	
Інтегральна компетентність	Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної та\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (ЗК)	**ЗК 1. Уміння критичної самооцінки** – здатність визначати та задовольняти потреби особистого та наукового розвитку, бути критичним і самокритичним. **ЗК 2. Навички творчого спілкування** – здатність спілкуватися результативно в усній і письмовій формах з фахівцями та нефахівцями, здатність спілкуватися другою мовою. **ЗК 3. Знання інформаційних технологій** – здатність використовувати інформаційні і комунікаційні технології для впровадження проектів в інформаційній та безпековій сферах. **ЗК 4. Навички керування проектами** – здатність демонструвати своєчасність та плановість у дослідженні, здатність до адаптації та дії в новій ситуації, здатність розробляти та управляти проектами. **ЗК 5.Уміння підтримати інших** – здатність допомагати через викладання, наставництво та наочні приклади (демонстрацію). **ЗК 6. Уміння працювати етично** – здатність визначати, поважати та керувати етичними, культурними та іншими питаннями, пов’язаними з наявністю тих чи інших відмінностей. **ЗК 7. Навички підприємництва** – здатність визначати підприємницькі можливості чи вид діяльності або громадського впливу, здатність приймати обґрунтовані рішення, здатність оцінювати та забезпечувати якість виконуваних робіт. **ЗК 8. Уміння командної роботи** – знання про стимули та бар’єри в ефективній командній роботі, вміння виявляти, ставити та вирішувати проблеми.
Фахові компетенції (ПП)	**ПП 1. Інтегративна компетентність** – здатність до інтеграції знань, умінь і навичок та їх ефективного використання в умовах швидкої адаптації організацій до вимог зовнішнього середовища, що забезпечують виконання завдань науково-дослідної, науково-педагогічної, управлінської та інноваційної діяльності в інформаційній та безпековій сфері тощо.

	ПП 2. Соціально-психологічна компетентність (емоційні, перцептивні, концептуальні, поведінкові) – здатність особистості орієнтуватися у різних життєвих ситуаціях, ефективно працювати в умовах ринкової економіки; уміння реалізувати стратегії і плани; здатність до розуміння поведінки людей, мотивації та організації їх спільної діяльності тощо. **ПП 3. Організаційно-комунікативна компетентність** (у специфічних сферах управлінської діяльності) – здатність до лідерства та новаторської діяльності, до формування високого рівня комунікативної культури; здатність переконувати оточуючих, стверджувати свою позицію; здатність до розробки проектів методичних і нормативних документів, до збирання та аналізу інформації, до прийняття управлінських рішень; володіння іноземними мовами, уміння правильно розмовляти та писати різними комунікативними стилями, а саме неофіційним, офіційним та науковим тощо. **ПП 4. Професійна компетентність** – стан теоретичної та практичної підготовленості, що забезпечує ефективність вирішення професійних проблем і нетипових професійних завдань; стан володіння інформаційними технологіями та технологіями захисту інформації; здатність до удосконалення та впровадження у практику сучасних ідей інформаційної та кібербезпеки, використання наукової літератури та інших джерел інформації для реалізації сучасних технологій тощо. **ПП 5. Загальнонаукова компетентність** – здатність до накопичення наукових знань та навичок (діагностування й інтерпретування ситуацій, планування та здійснення наукових досліджень, що відносяться до галузі інформаційних технологій та захисту інформації); здатність до генерування нових знань з теорії захисту інформації та інформаційної безпеки, з проблем проектування та застосування засобів та комплексів технічного захисту інформації; тощо. **ПП 6. Політехнічна компетентність** – здатність до оволодіння сучасними інформаційними технологіями

	для рішення експериментальних і практичних завдань в галузі інформаційної безпеки, вести розробку алгоритмів, програм та конструкторської документації, налагодження, макетування засобів технічного захисту інформації з обмеженим доступом та пристроїв внутрішньооб'єктового контролю, представляти результати роботи й обґрунтовувати запропоновані рішення на сучасному науково-технічному й професійному рівні. **ПП 7. Інженерна компетентність** – здатність до виробничо-технологічної діяльності (використовуючи технічні засоби захисту інформації в умовах забезпечення режиму секретності на підприємствах, в організаціях та установах різних форм власності, уміти провести дії щодо організації технічного захисту інформації); здатність до організаційно-управлінської діяльності (добору й аналізу відповідної інформації щодо розв'язання ситуаційних проблем, які виникають у сфері забезпечення інформаційної безпеки); здатність до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення режиму секретності на підприємствах, установах, організаціях з різними формами власності, уміти провести дії щодо організації та впровадження систем технічного захисту інформації тощо. **ПП 8. Ділова компетентність** – здатність до планування й реалізації заходів обліку та атестації території та об'єктів, підприємств, установ, організацій; створення та забезпечення функціонування систем інформаційної та кібербезпеки; здатність до формування правильних висновків, оперативного приймання та реалізації нестандартних рішень тощо.
7 – Програмні результати навчання	
	ПРН 1. Уміти формувати і аргументовано відстоювати власну позицію з різних проблем філософії науки та методології наукового пізнання. Бути критичним і самокритичним. Вирішувати завдання з проблем самоактуалізації особистості, саморозвитку, самоосвіти, самовиховання та самоорганізації. **ПРН 2.** Уміти читати оригінальну наукову літературу на іноземній мові, опрацьовувати та оформляти інформацію.

	ПРН 3. Уміти розробляти логічні схеми, складати план-проспекти та технічні завдання на виконання наукових досліджень. Здійснювати бібліографічний пошук і відбір літературних джерел, складати їх бібліографічний опис. **ПРН 4. Уміти приймати** обґрунтовані рішення, бути здатним їх оцінювати та забезпечувати якість виконуваних робіт, володіти предметною базою знань та сучасними техніками дослідження, здатність створювати та інтерпретувати нові знання. **ПРН 5. Уміти** за результатами обстеження, обліку та атестації території та об'єктів, підприємств, установ, організацій визначати канали можливого витоку інформації. **ПРН 6. Уміти** розробляти документацію (звіти, структурні, функціональні, принципові, конструкторські схеми тощо), необхідну для супроводу систем технічного захисту інформації. **ПРН 7. Уміти** розробляти, організовувати розроблення та здійснювати побудову системи організаційно-службових та спеціальних заходів із забезпечення інформаційної безпеки установ, підприємств, організацій. **ПРН 8. Уміти** аналізувати інформацію, надану технічними системами, з метою виявлення ознак можливого несанкціонованого доступу до інформації. **ПРН 9. Бути здатним** забезпечувати заходи та засоби охорони праці та техніки безпеки під час робіт на спорудах та обладнанні інформаційних та інформаційно-комунікаційних засобів, використовуючи нормативні документи та наявні матеріально-технічні ресурси, знання основ техніки безпеки та основ охорони праці. **ПРН 10.** Бути зданим розробляти та проводити експериментальні дослідження перспективних засобів та комплексів технічного захисту інформації, проводити випробування та обробляти результати експериментів. **ПРН 11.** Бути зданим проводити аналіз та моделювання процесів, що відбуваються в технічних об'єктах, пристроях та їх компонентах в системах технічного захисту інформаці. **ПРН 12.** Уміти підбирати такі моделі об'єктів і пристроїв систем технічного захисту інформації, які підходять для

	рішення складних задач технічного захисту інформації. **ПРН 13.** Бути зданим проводити дослідження алгоритмів і програм, розв'язувати задачі статичного і динамічного планування в комп'ютерних системах, підбирати такі методи, моделі і алгоритми, що забезпечують оптимальне розв'язання задач захисту інформації підприємств, установ, організацій. **ПРН 14. Уміти** розробляти схему розташування (підключення) технічних засобів внутрішньо-об'єктового контролю та перепускного режиму та **бути зданим** забезпечити ефективне функціонування пристроїв і систем технічного захисту інформації. **ПРН 15. Бути зданим** провести переконливе обґрунтування або ж аргументовано вказати на недоцільність(суперечливість) дій щодо організації та впровадження технічного захисту інформації. **ПРН 16. Уміти** складати виписки із нормативної та службової документації для передавання їх відповідальним особам, що задіяні у проведенні службових розслідувань. **ПРН 17. Уміти** оцінити повноту та досконаліть плану заходів для запобігання розголошення чи витоку відомостей, документації, іншої інформації обмеженого доступу під час виконання робіт по забезпеченню встановлення та запуску в експлуатацію системами захисту від несанкціонованого доступу до інформаційних ресурсів обмеженого доступу. **ПРН 18. Уміти** розробляти та визначати показники рівня безпеки об'єкта управління інформаційною безпекою на підприємстві (в установі, організації) на найближчу і віддалену перспективу на основі існуючого стану справ за умови наявних ресурсів. **ПРН 19. Уміти** розробляти, організовувати розроблення та здійснювати побудову системи організаційно-службових та спеціальних заходів із забезпечення інформаційної безпеки установ, підприємств, організацій. **ПРН 20. Уміти** застосовувати системний підхід до розробки комплексу організаційних заходів та розробляти нормативно-методичні матеріали з організації захисту інформації враховуючи особливості функціонування підприємства та вирішуваних ним завдань.

8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Висококваліфікований науково-педагогічний склад
Матеріально-технічне забезпечення	Теоретичні заняття проводяться в сучасних комп'ютерних класах та спеціалізованих лабораторіях, які оснащені спеціалізованими апаратно-програмними засобами.
Інформаційне та навчально-методичне забезпечення	Всі дисципліни навчального плану забезпечені інформаційними та навчально-методичними матеріалами, у т.ч. засобами системи дистанційного навчання Moodle.
9 – Академічна мобільність	
Національна кредитна мобільність	Наявність двосторонніх договорів між ДУТ та вищими навчальними закладами 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 / наукової 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				
2.	Групова динаміка і комунікації	ЗК12.1.01	ЗК 1, ЗК 5, ЗК 8, ПП 1	ПРН 1, ПРН 2, ПРН 4
3.	Ділові комунікації	ЗК12.1.02	ЗК 2, ЗК 5, ПП 2	ПРН 1, ПРН 2, ПРН 4
4.	Філософія	ЗК12.1.03	ЗК 1, ЗК 2, ЗК 5, ЗК 6, ПП 2	ПРН 1
5.	Засади відкриття власного бізнесу	ЗК12.1.04	ЗК 4, ЗК 5, ЗК 7, ПП 1	ПРН 4, ПРН 9, ПРН 16, ПРН 20
6.	Іноземна мова*	ЗК12.1.05	ЗК 1, ПП 3	ПРН 2
7.	Вища математика	ЗК12.1.06	ЗК 6, ПП 4	ПРН 8
8.	Нормативно-правове забезпечення інформаційної безпеки	ЗК12.1.07	ЗК 8, ПП 4	ПРН 4, ПРН 9, ПРН 16, ПРН 20
9.	Соціально-екологічна безпека життєдіяльності	ЗК12.1.08	ЗК 6, ПП 1	ПРН 9
10.	Застосування інформаційно-телекомунікаційних засобів	ЗК12.1.09	ЗК 1, ЗК 2, ПП 2, ПП 7	ПРН 7, ПРН 10, ПРН 11, ПРН 14
11.	Фізика	ЗК12.1.10	ЗК 1, ЗК 2, ПП 1	ПРН 8
12.	Теорія інформації та кодування	ЗК12.1.11	ЗК 3, ПП 1, ПП 2, ПП 6, ПП 7	ПРН 3, ПРН 5
13.	Фізичні поля як носії інформації	ЗК12.1.12	ЗК 3, ПП 1, ПП 2, ПП 6, ПП 7	ПРН 3, ПРН 5
2. Цикл дисциплін професійної та практичної підготовки				
2.1. Дисципліни спеціальності				
1.	Теорія кіл і сигналів в інформаційному та кіберпросторах	ПП12.2.01	ЗК 3, ПП 1, ПП 2, ПП 6, ПП 7	ПРН 3, ПРН 5,
2.	Прикладне програмування	ПП12.2.02	ЗК 4, ПП 5, ПП 6	ПРН 8, ПРН 12
3.	Апаратні та програмні засоби комп'ютерної інженерії	ПП12.2.03	ЗК 3, ПП 1, ПП 4, ПП 5, ПП 7	ПРН 5, ПРН 7, ПРН 9, ПРН 10, ПРН 11
4.	Операційні системи	ПП12.2.04	ЗК 3, ПП 1, ПП 4, ПП 5, ПП 7	ПРН 5, ПРН 7, ПРН 10, ПРН 12

5.	Комп'ютерні мережі	ПП12.2.05	ЗК 3, ЗК 4, ПП 1, ПП 4, ПП 5, ПП 7, ПП 8	ПРН 5, ПРН 7, ПРН 9, ПРН 11, ПРН 14
6.	Стандарти інформаційної та кібербезпеки	ПП12.2.06	ЗК 3, ПП 6, ПП 7, ПП 8	ПРН 4, ПРН 16, ПРН 17, ПРН 19
7.	Прикладна криптологія	ПП12.2.07	ЗК 3, ПП 6, ПП 7, ПП 8	ПРН 8, ПРН 17, ПРН 18
8.	Аудит систем захисту інформації	ПП12.2.08	ЗК 3, ПП 6, ПП 7, ПП 8	ПРН 4, ПРН 6, ПРН 15
9.	Хмарні технології	ПП12.2.09	ЗК 3, ПП 1, ПП 4, ПП 5	ПРН 14
10.	Комплексні системи захисту інформації	ПП12.2.10	ЗК 3, ЗК 4, ПП 5, ПП 6, ПП 7, ПП 8	ПРН 3, ПРН 4, ПРН 5, ПРН 6, ПРН 7, ПРН 9, ПРН 13, ПРН 14, ПРН 16, ПРН 19
11.	Штучний інтелект	ПП12.2.11	ЗК 3, ПП 1, ПП 4, ПП 5	ПРН 10, ПРН 15, ПРН 16
2.2. Дисципліни фахової спеціальності				
1.	Компонентна база в системах захисту інформації	ПП12.2.12	ПП 5, ПП 6, ПП 7	ПРН 5, ПРН 6, ПРН 7, ПРН 11, ПРН 12
2.	Поля і хвилі в системах технічного захисту інформації	ПП12.2.13	ЗК 3, ПП 4, ПП 5, ПП 6, ПП 7, ПП 8	ПРН 3, ПРН 4, ПРН 5, ПРН 13
3.	Засоби передачі в системах технічного захисту інформації	ПП12.2.14	ЗК 3, ПП 5, ПП 6, ПП 7, ПП 8	ПРН 6, ПРН 7, ПРН 10, ПРН 15
4.	Засоби прийому та обробки сигналів в системах технічного захисту інформації	ПП12.2.15	ЗК 3, ПП 5, ПП 6, ПП 7, ПП 8	ПРН 6, ПРН 16
5.	Методи та засоби технічного захисту інформації	ПП12.2.16	ЗК 3, ПП 4, ПП 6, ПП 7, ПП 8	ПРН 5, ПРН 8, ПРН 12
6.	Схемотехніка пристроїв технічного захисту інформації	ПП12.2.17	ЗК 3, ПП 4, ПП 6, ПП 7	ПРН 6, ПРН 12, ПРН 14
7.	Безпека безпроводових, мобільних та хмарних технологій	ПП12.2.18	ЗК 3, ПП 4, ПП 5, ПП 6, ПП 7, ПП 8	ПРН 6, ПРН 7, ПРН 9, ПРН 11, ПРН 12, ПРН 13, ПРН 14, ПРН 16
8.	Метрологія та вимірювання в ІБ	ПП12.2.19	ПП 5, ПП 6, ПП 7, ПП 8	ПРН 6, ПРН 7, ПРН 14, ПРН 15, ПРН 16, ПРН 19

9.	Технічні засоби охорони обєктів	ПП12.2.20	ЗК 3, ПП 4, ПП 5, ПП 6, ПП 7, ПП 8	ПРН 8, ПРН 12, ПРН 16, ПРН 17, ПРН 18
10.	Менеджмент інформаційної безпеки	ПП12.2.21	ЗК 4, ЗК 5, ПП 1, ПП 2, ПП 3	ПРН 1, ПРН 13, ПРН 16, ПРН 19, ПРН 20
11.	Ознайомча практика	ПП12.2.22	ЗК 3, ЗК 6, ПП 3, ПП 4, ПП 7	ПРН 1, ПРН 7, ПРН 9, ПРН 11
12.	Виробнича практика	ПП12.2.23	ЗК 3, ЗК 6, ПП 3, ПП 4, ПП 7	ПРН 1, ПРН 7, ПРН 9 , ПРН 11
13.	Переддипломна практика	ПП12.2.24	ЗК 7, ПП 5, ПП 6, ПП 7, ПП 8	ПРН 1, ПРН 7, ПРН 9, ПРН 10, ПРН 11,
14.	Кваліфікаційна робота	ПП12.2.25	ЗК 6, ЗК 7, ПП 5, ПП 6, ПП 7, ПП 8	ПРН 1, ПРН 2, ПРН 7 , ПРН 10, ПРН 11
15.	Підсумкова атестація			
3. Дисципліни вільного вибору студента				
3.1. Дисципліни циклу загальної підготовки				
1.	Іноземна мова*	ППк 12.3.01.01	ЗК 1, ПП 1, ПП 2, ПП 3	ПРН 2,
2.	Іноземна мова професійного спрямування*	ППк 12.3.01.02	ЗК 1, ПП 1, ПП 2, ПП 3, ПП 4,	ПРН 1, ПРН 2.
2.2. Дисципліни циклу професійної та практичноїпідготовки				
3.	Захист від шкідливого програмного засобу	ППк 12.3.2.1	ЗК 3, ПП 2, ПП 3, ПП 4, ПП 7	ПРН 6, ПРН 12, ПРН 13
4.	*Інженерна та компютерна графіка*	ППк 12.3.2.2	ЗК 3, ПП 1, ПП 6	ПРН 7
5.	Аналіз та оцінка уразливостей інформаційних систем	ППк 12.3.2.3	ЗК 3, ПП 1, ПП 3, ПП 4, ПП 5	ПРН 6, ПРН 13
6.	*Перспективні компоненти та засоби інфокомунікаційних технологій*	ППк 12.3.2.4	ЗК 3, ПП 1, ПП 7	ПРН 7, ПРН 9, ПРН 10

7.	Програмні комплекси захисту автоматизованих систем від несанкціонованого доступу	ППк 12.3.2.5	ЗК 3, ПП 3, ПП 4, ПП 5, ПП 6, ПП 7, ПП 8	ПРН 6, ПРН 9, ПРН 13
8.	*Сучасні комп'ютерні системи та мережі*	ППк 12.3.2.6	ЗК 3, ПП 3, ПП 4	ПРН 7, ПРН 9, ПРН 10, ПРН 14
9.	Проектування систем технічного захисту інформації	ППк 12.3.2.7	ЗК 3, ПП 5, ПП 6, ПП 7, ПП 8	ПРН 5, ПРН 6, ПРН 9, ПРН 10, ПРН 14
10.	*Системи управління електронним документообігом*	ППк 12.3.2.8	ЗК 3, ПП 3, ПП 4	ПРН 7, ПРН 20
11.	Кібербезпека банківських та комерційних структур	ППк 12.3.2.9	ЗК 4, ПП 3, ПП 4, ПП 5, ПП 6, ПП 7, ПП 8	ПРН 6, ПРН 9, ПРН 13, ПРН 20
12.	*Комп'ютерні технології вимірювань в телекомунікаціях*	ППк 12.3.2.10	ЗК 3, ПП 3, ПП 4	ПРН 7, ПРН 9, ПРН 10, ПРН 14
13.	Цифрова криміналістика	ППк 12.3.2.11	ЗК 4, ПП 3, ПП 4, ПП 5, ПП 6, ПП 7, ПП 8	ПРН 6, ПРН 7
14.	*Інформаційні ресурси та сервіси в інфокомунікаціях*	ППк 12.3.2.12	ЗК 3, ПП 3, ПП 4, ПП 7	ПРН 7, ПРН 9, ПРН 10, ПРН 14

***** *Для іноземців та осіб без громадянства замінюється на дисципліну «Українська мова»*

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	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 інформаційної безпеки	3	Іспит
ЗК12.1.08	Соціально-екологічна безпека життєдіяльності	3	Іспит
ЗК12.1.09	Застосування інформаційно-телекомунікаційних засобів	6	Залік
ЗК12.1.10	Фізика	7	Залік, Іспит
ЗК12.1.11	Теорія інформації та кодування	4	Іспит

ЗК12.1.12	Фізичні поля як носії інформації	3	Іспит
Загальний обсяг обов'язкових компонент:		60	
1. Цикл дисциплін професійної та практичної підготовки			
1.1. Дисципліни спеціальності			
ПП12.2.01	Теорія кіл і сигналів в інформаційному та кіберпросторах	5	Іспит Курсовий проект
ПП12.2.02	Прикладне програмування	10	Залік, Іспит Курсовий проект
ПП12.2.03	Апаратні та програмні засоби комп'ютерної інженерії	5	Залік
ПП12.2.04	Операційні системи	6	Іспит
ПП12.2.05	Комп'ютерні мережі	4	Іспит
ПП12.2.06	Стандарти інформаційної та кібербезпеки	3	Залік
ПП12.2.07	Прикладна криптологія	8	Залік, Іспит Курсовий проект
ПП12.2.08	Аудит систем захисту інформації	3	Залік
ПП12.2.09	Хмарні технології	3	Залік
ПП12.2.10	Комплексні системи захисту інформації	10	Залік, Іспит Курсовий проект
ПП12.2.11	Штучний інтелект	3	Залік
ПП12.2.12	Компонентна база в системах захисту інформації	3	Залік
ПП12.2.13	Поля і хвилі в системах технічного захисту інформації	7	Залік, Іспит Курсовий проект
ПП12.2.14	Засоби передачі в системах технічного захисту інформації	4	Залік
ПП12.2.15	Засоби прийому та обробки сигналів в системах технічного захисту інформації	4	Залік
ПП12.2.16	Методи та засоби технічного захисту інформації	4	Залік
ПП12.2.17	Схемотехніка пристроїв технічного захисту інформації	3	Іспит
ПП12.2.18	Безпека безпроводових, мобільних та хмарних технологій	4	Залік
ПП12.2.19	Метрологія та вимірювання в ІБ	4	Іспит
ПП12.2.20	Технічні засоби охорони обєктів	3	Іспит
ПП12.2.21	Менеджмент інформаційної безпеки	3	Залік
ПП12.2.22	Ознайомча практика	3	Залік
ПП12.2.23	Виробнича практика	6	Залік
ПП12.2.24	Переддипломна практика	6	Залік
ПП12.2.25	Кваліфікаційна робота	5	
	Підсумкова атестація	1	
Загальний обсяг обов'язкових компонент:		**180**	
Вибіркові компоненти ОП			
Вибірковий блок 1 (за вибором студентів)			
ППк 12.3.01.01	Іноземна мова	10	Залік, Іспит
ППк 12.3.01.02	Іноземна мова професійного спрямування	20	Залік, Іспит
ППк	Військова підготовка	30	

12.3.01.03			
Вибірковий блок 2(за вибором студентів)			
ППк 12.3.2.1	Захист від шкідливого програмного засобу	5	Залік
ППк 12.3.2.2	*Інженерна та компютерна графіка*		
ППк 12.3.2.3	Аналіз та оцінка уразливостей інформаційних систем	5	Іспит
ППк 12.3.2.4	*Перспективні компоненти та засоби інфокомунікаційних технологій*		
ППк 12.3.2.5	Програмні комплекси захисту автоматизованих систем від несанкціонованого доступу	5	Іспит
ППк 12.3.2.6	*Сучасні комп'ютерні системи та мережі*		
ППк 12.3.2.7	Проектування систем технічного захисту інформації	5	Іспит
ППк 12.3.2.8	*Системи управління електронним документообігом*		
ППк 12.3.2.9	Кібербезпека банківських та комерційних структур	5	Іспит
ППк 12.3.2.10	*Комп'ютерні технології вимірювань в телекомунікаціях*		
ППк 12.3.2.11	Цифрова криміналістика	5	Іспит
ППк 12.3.2.12	*Інформаційні ресурси та сервіси в інфокомунікаціях*		
Загальний обсяг вибіркових компонент:		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

2.3. Структурно-логічна схема ОП

Цикл	I курс				Всього	
	1 семестр		2 семестр		Кр.	%
Цикл загальної підготовки	Іноземна мова	5	Іноземна мова	5		
	Вища математика	4	Вища математика	4		
	Нормативно-правове забезпечення інформаційної безпеки	3	Групова динаміка і комунікації	3		
	Застосування інформаційно-телекомунікаційних засобів	6	Соціально-екологічна безпека життєдіяльності	3		
	Фізика	4	Фізика	3		
	Всього	***22***	***Всього***	***18***		
Цикл професійної підготовки	Теорія кіл і сигналів в інформаційному та кіберпросторах	5	Апаратні та програмні засоби комп'ютерної інженерії	5		
	Прикладне програмування	3	Прикладне програмування	7		
	Всього	***30***	***Всього***	***30***		
	Всього за I курс				**60**	**25**

Цикл	2 курс				Всього	
	3 семестр		4 семестр		Кр.	%
Цикл загальної підготовки	Вища математика	4	Ділові комунікації	3		
	Теорія інформації та кодування	4	Філософія	3		
	Фізичні поля як носії інформації	3				
	Всього	***11***	***Всього***	***6***		
Цикл професійної підготовки	Операційні системи	6	Комп'ютерні мережі	4		
	Стандарти інформаційної та кібербезпеки	3	Прикладна криптологія	4		
			Компонентна база в системах захисту інформації	3		
			Ознайомча практика	3		
	Всього	***9***	***Всього***	***14***		

Вільного вибору студента	Іноземна мова	5	Іноземна мова	5		
	Захист від шкідливого програмного засобу	5	Аналіз та оцінка уразливостей інформаційних систем	5		
	Інженерна та компютерна графіка		*Перспективні компоненти та засоби інфокомунікаційних технологій*			
	Всього	***10***	***Всього***	***10***		
	Всього за 2 курс				**60**	**25**
Цикл	**3 курс**				Всього	
	5 семестр		**6 семестр**		Кр.	%
Цикл загальної підготовки						
	Всього		***Всього***			
Цикл професійної підготовки	Прикладна криптологія	4	Аудит систем захисту інформації	3		
	Поля і хвилі в системах технічного захисту інформації	4	Поля і хвилі в системах технічного захисту інформації	3		
	Засоби передачі в системах технічного захисту інформації	4	Засоби прийому та обробки сигналів в системах технічного захисту інформації	4		
	Методи та засоби технічного захисту інформації	4	Схемотехніка пристроїв технічного захисту інформації	4		
	Безпека безпроводових, мобільних та хмарних технологій	4	Виробнича практика	6		
	Всього	***20***	***Всього***	***20***		
Вільного вибору студента	Іноземна мова професійного спрямування	5	Іноземна мова професійного спрямування	5		
	Програмні комплекси захисту автоматизованих систем від несанкціонованого доступу	5	Проектування систем технічного захисту інформації	5		
	Сучасні комп'ютерні системи та мережі		*Системи управління електронним документообігом*			
	Всього	***10***	***Всього***	***10***		
	Всього за 3 курс				**60**	**25**
Цикл	**4 курс**				Всього	
	7 семестр		**8 семестр**		Кр.	%
Цикл загальної підготовки	Засади відкриття власного бізнесу	3				

	Всього	***3***	***Всього***		**3**	
Цикл професійної підготовки	Хмарні технології	3	Штучний інтелект	3		
	Комплексні системи захисту інформації	5	Комплексні системи захисту інформації	5		
	Технічні засоби охорони обєктів	3	Переддипломна практика	6		
	Метрологія та вимірювання в ІБ	3	Кваліфікаційна робота Підсумкова атестація	6		
	Менеджмент інформаційної безпеки	3				
	Всього	***20***	***Всього***	***20***		
Вільного вибору студента	Іноземна мова професійного спрямування	5	Іноземна мова професійного спрямування	5		
	Кібербезпека банківських та комерційних структур	5	Цифрова криміналістика	5		
	Комп'ютерні технології вимірювань в телекомунікаціях		*Інформаційні ресурси та сервіси в інфокомунікаціях*			
	Всього	***10***	***Всього***	***10***		
	Всього за 4 курс				**60**	**25**
Всього					**240**	**100**

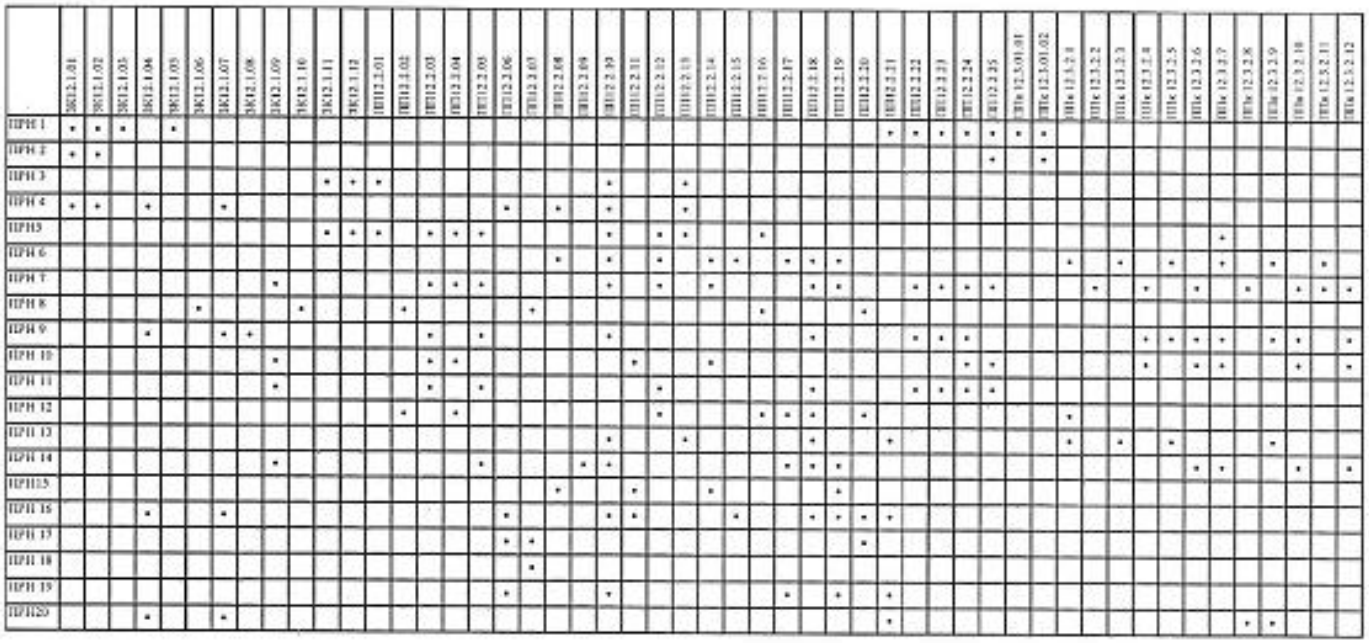
3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація бакалаврів з кібербезпеки здійснюється у формі публічного захисту бакалаврської роботи.
Вимоги до кваліфікаційної роботи	Атестація здійснюється відкрито і гласно. Кваліфікаційна робота перевіряється на плагіат згідно «Положення про запобігання академічному плагіату у Державному університеті телекомунікацій»

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ЗКІ2.1.01	ЗКІ2.1.02	ЗКІ2.1.03	ЗКІ2.1.04	ЗКІ2.1.05	ЗКІ2.1.06	ЗКІ2.1.07	ЗКІ2.1.08	ЗКІ2.1.09	ЗКІ2.1.10	ЗКІ2.1.11	ЗКІ2.1.12	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	ШКв 12.3.01.01	ШКв 12.3.01.02	ШКв 12.3.2.1	ШКв 12.3.2.2	ШКв 12.3.2.3	ШКв 12.3.2.4	ШКв 12.3.2.5	ШКв 12.3.2.6	ШКв 12.3.2.7	ШКв 12.3.2.8	ШКв 12.3.2.9	ШКв 12.3.2.10	ШКв 12.3.2.11	ШКв 12.3.2.12
ЗК 1	•		•		•				•	•																											•	•												
ЗК 2		•	•						•	•																																								
ЗК 3											•	•	•		•	•	•	•	•	•	•	•	•		•	•	•	•		•		•		•	•				•	•	•	•	•	•		•		•		•
ЗК 4				•										•			•					•											•														•		•	
ЗК 5	•	•	•	•																													•																	
ЗК 6			•			•		•																										•	•		•												
ЗК 7				•																																•	•												
ЗК 8	•						•																																											
ПП 1	•			•				•		•	•	•	•		•	•	•				•		•						•				•				•	•			•	•	•						
ПП 2		•	•						•		•	•	•																				•				•	•	•											
ПП 3					•																												•	•	•		•	•	•			•		•	•		•	•	•	•
ПП 4						•	•								•	•	•				•		•		•		•	•	•	•		•		•	•		•	•	•			•		•	•		•	•	•	•
ПП 5														•	•	•	•				•	•	•	•	•	•		•	•	•	•	•				•	•				•		•		•		•		
ПП 6											•	•	•	•				•	•	•		•		•	•	•	•	•	•	•	•	•				•	•			•			•		•		•		
ПП 7									•		•	•	•		•	•	•	•	•	•		•		•	•	•	•	•	•	•	•	•	•	•		•	•				•		•		•		•	•	•
ПП 8																	•	•	•	•		•			•	•		•	•	•	•	•				•	•				•		•		•		•		

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



Гарант освітньої програми

Доцент кафедри систем захисту інформації
кандидат технічних наук, доцент

О. В. Труш