**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 № 15 від 25 березня 2019 р.
Освітня програма вводиться в дію з 01.09.2019 р.

Виконувач обов'язків ректора
_____ Л.Н. Беркман
Наказ № 152 від 25 березня 2019 р.

Київ 2019

**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 № 3 від 21 березня 2019 року

Голова науково-методичної ради _____ Л.Н.Беркман

2. Проректор з навчальної роботи _____ А.М. Явтушенко

3. Директор навчально-наукового центру _____ В.В. Гуменюк

4. Вчена рада Навчально-наукового інституту захисту інформації
протокол № 8 від “19” березня 2019 року

Голова вченої ради інституту _____ С.В. Довбешко

5. Кафедра систем інформаційного та кібернетичного захисту
протокол № 10 від “ 18 ” березня 2019 року

Завідувач кафедри _____ В.А. Савченко

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

1. Науково-дослідна установа «Інститут кібербезпеки».

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

**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 кібербезпеки* |
| **професійна кваліфікація** | *3439 Фахівець із організації захисту інформації з обмеженим доступом* |

6. Представник професійної асоціації (ринку праці)

Директор Науково-дослідної установи «Інститут кібербезпеки»

_____ С.С. Туранська

7. Представник професійної асоціації (ринку праці)

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

_____ А.О. Фесенко

**«ПОГОДЖЕНО»**

Науково-дослідна установа «Інститут кібербезпеки»

_____ С.С. Туранська

МП

«_____» _____ 201__р.

**«ПОГОДЖЕНО»**

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

_____ А.О. Фесенко

МП

«_____» _____ 201__р.

# ПЕРЕДМОВА

Розроблено проектною групою Навчально-наукового інституту захисту інформації Державного університету телекомунікацій (склад проектної групи затверджено наказом ректора університету № 91 від 20.02.2019 р.) у складі:

**Керівник – Савченко Віталій Анатолійович** – завідувач кафедри систем інформаційного та кібернетичного захисту Навчально-наукового інституту захисту інформації Державного університету телекомунікацій, доктор технічних наук з спеціальності 122 Комп'ютерні науки та інформаційні технології (05.13.06 - інформаційні технології), старший дослідник за спеціальністю 20.02.14 – озброєння та військова техніка.

**Члени проектної групи:**

**Довбешко Станіслав Володимирович** – директор Навчально-наукового інституту захисту інформації Державного університету телекомунікацій, кандидат технічних наук з спеціальності 255 Озброєння та військова техніка (20.02.14 - озброєння та військова техніка), доцент за кафедрою схемотехніки радіоелектронних систем.

**Ахрамович Володимир Миколайович** - доцент кафедри систем інформаційного та кібернетичного захисту Навчально-наукового інституту захисту інформації Державного університету телекомунікацій, кандидат технічних наук з спеціальності 131 Прикладна механіка (05.03.01 - процеси механічної та фізико-технічної обробки, верстати та інструменти), доцент кафедри технологій виробництва та капітального ремонту озброєння військової техніки.

Освітньо-професійна програма приведена у відповідність державним стандартам вищої освіти зі спеціальності 125 Кібербезпека, затвердженим наказом Міністерства освіти і науки України від 04.10.2018 р. № 1074.

## 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<br>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;<br>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);<br>на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційний рівень «молодший спеціаліст») – обсяг освітньої програми більше 120 кредитів ЄКТС при перезарахуванні не більше 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки |
| **Наявність акредитації** | Сертифікат про акредитацію спеціальності 125 Кібербезпека НД № 1190091 від 21.08.17 р. Термін дії сертифікату 01.07. 2018 р. Проведена чергова акредитація у лютому 2019 року. |
| **Цикл/рівень** | НРК України – 6 рівень/ Бакалавр,<br>QF-EHEA- перший цикл,<br>EQF-LLL – 6 рівень |
| **Передумови** | наявність атестата про середню освіту або диплома молодшого бакалавра (освітньо-кваліфікаційний рівень «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/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<br>125 Кібербезпека |
| **Орієнтація освітньої програми** | Освітньо-професійна. 100% обсягу освітньо-професійної програми спрямовано на забезпечення загальних та спеціальних (фахових компетентностей за спеціальністю 125 Кібербезпека 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.<br>Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та кібербезпеки на підприємствах в установах та організаціях.<br>Ключові слова: ІНФОРМАЦІЯ, ЗАГРОЗИ, ВРАЗЛИВОСТІ, ЗАХИЩЕНІСТЬ, КІБЕРБЕЗПЕКА, ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ. |
| **Опис предметної області** | **Об'єкти професійної діяльності випускників**:<br>об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології;<br>технології забезпечення безпеки інформації;<br>процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту.<br>**Цілі навчання** підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки .<br>**Теоретичний зміст предметної діяльності**<br>Знання: законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і |

| | |
|---|---|
| | практик щодо здійснення професійної діяльності;<br>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.<br>**Методи, методики та технології:**<br>Методи, методики інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки<br>**Інструменти та обладнання:**<br>системи розробки, забезпечення, моніторингу та контролю інформаційної та/ або кібербезпеки;<br>сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. |
| **Особливості програми** | Програма передбачає:<br>Програма передбачає:<br>- викладання окремих дисциплін циклу професійної підготовки англійською мовою;<br>- передбачено в межах освітнього процесу поглиблене вивчення студентами найбільш важливих тем на навчальній базі компаній-партнерів з подальшим одержанням сертифікатів, зокрема: «Introduction to Cybersecurity» від компанії Cisco; «Стандарт ISO/IEC 27001, практичні аспекти проведення аудиту» від компанії Bureau Veritas Ukraine; «HP ATA Networks» від компанії Hewlett Packard; «Інженер-налагоджувальник обладнання HikVision» та «Біометрія ZKTeco» від компанії Інфотех;<br>- залучення до проведення, семінарських, практичних занять та лабораторних робіт, фахівців-практиків з інформаційної безпеки.<br>- забезпечення умов підготовки здобувачів вищої освіти у реальному середовищі майбутньої професійної діяльності для набуття відповідних компетенцій, шляхом організації проведення практик (навчальна, виробнича та переддипломна) на фірмах-партнерів, серед яких: міжнародні корпорації (IBM, Cisco), державні підприємства України («Державний центр |

| | |
|---|---|
| | кіберзахисту та протидії кіберзагрозам», «Українські спеціальні системи», «Український центр «Безпека»); науково-дослідні інститути (Автопром, Електромагнітні прилади, Криптон); комерційні організації (ESET, Ajax-Systems, Автор, Епос, Інфозахист, Інформатика, Інфотех); приватні підприємства (Ріас, НомерОК), з можливістю подальшого працевлаштування. |
| **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:<br>**Основна:**<br>*3439 Фахівець із організації захисту інформації з обмеженим доступом*<br>**Додаткова:**<br>3439 Фахівець з організації інформаційної безпеки<br>3121 Фахівець з інформаційних технологій<br>3114 Фахівець інфокомунікацій<br>3119 Технік (сфера захисту інформації) |
| **Подальше навчання** | Можливість продовжити навчання за освітньою програмою другого (магістерського) освітнього рівня. Набуття додаткових кваліфікацій в системі післядипломної освіти. |
| **5 – Викладання та оцінювання** | |
| **Викладання та навчання** | Викладання проводиться державною мовою. Іноземною мовою (англійською) проводиться викладання окремих дисциплін, які формують професійні компетентності. Викладання спрямовано на засвоєння знань, умінь і навичок для подальшого застосування на практиці.<br>Основними способами передачі змісту освітньої програми є проведення лекцій, практичних, лабораторних та індивідуальних занять, консультацій, розв’язання ситуативних завдань, тестування, презентацій, ознайомча, виробнича, переддипломна практики. |
| **Оцінювання** | Оцінювання сформованих компетенцій проводиться під час контрольних заходів, які передбачені цією освітньою програмою та зазначені у навчальному плані. Критерії оцінювання знань, умінь та навичок здобувачів вищої освіти розроблені у відповідності до чинного законодавства та затверджені у «Положенні про організацію освітнього процесу у Державному університеті телекомунікацій». |

| 6- Програмні компетенції | |
|---|---|
| **Інтегральна компетентність** | Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної та кібербезпеки, що характеризується комплексністю та неповною визначеністю умов. |
| **Загальні компетентності (ЗК)** | **ЗК 1.** Здатність застосовувати знання у практичних ситуаціях.<br>**ЗК 2.** Знання та розуміння предметної області та розуміння професії.<br>**ЗК 3.** Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.<br>**ЗК 4.** Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.<br>**ЗК 5.** Здатність до пошуку, оброблення та аналізу інформації.<br>**ЗК 6.** Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного)суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина і Україні.<br>**ЗК 7.** Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. |
| **Фахові компетенції (ПП)** | **ПП 1.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та кібербезпеки.<br>**ПП 2**. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки.<br>**ПП 3.** Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.<br>**ПП 4.** Здатність забезпечувати неперервність бізнесу згідно встановленої політики безпеки.<br>**ПП 5.** Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних |

| | |
|---|---|
| | (автоматизованих) системах з метою реалізації встановленої політики безпеки.<br>**ПП 6.** Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.<br>**ПП 7.** Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) .<br>**ПП 8.** Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.<br>**ПП 9.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою.<br>**ПП 10.** Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.<br>**ПП 11.** Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем.<br>**ПП 12**. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам. |
| **7 – Програмні результати навчання** | |
| | **ПРН 1.** Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.<br>**ПРН 2.** Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблему професійній діяльності, оцінювати їхню ефективність.<br>**ПРН 3.** Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.<br>**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.<br>**ПРН 5.** Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.<br>**ПРН 6.** Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.<br>**ПРН 7.** Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, тому числі міжнародних в галузі інформаційної та кібербезпеки.<br>**ПРН 8.** Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та кібербезпеки.<br>**ПРН 9.** Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та кібербезпеки.<br>**ПРН 10.** Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.<br>**ПРН 11.** Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.<br>**ПРН 12.** Розробляти моделі загроз та порушника.<br>**ПРН 13.** Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.<br>**ПРН 14.** Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку якості прийнятих рішень.<br>**ПРН 15.** Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.<br>**ПРН 16.** Реалізовувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативно-правових документів.<br>**ПРН 17.** Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент. |

| | |
|---|---|
| | **ПРН 18.** Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.<br>**ПРН 19**. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.<br>**ПРН 20.** Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в ІТС.<br>**ПРН 21.** Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.<br>**ПРН 22.** Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної та кібербезпеки.<br>**ПРН 23.** Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.<br>**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).<br>**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.<br>**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.<br>**ПРН 27**. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.<br>**ПРН 28**. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних |

| | |
|---|---|
| | (автоматизованих) системах згідно встановленої політики інформаційної та кібербезпеки.<br>**ПРН 29.** Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.<br>**ПРН 30.** Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.<br>**ПРН 31.** Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.<br>**ПРН 32.** Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.<br>**ПРН 33.** Вирішувати задачі забезпечення неперервності бізнес процесів організації.<br>**ПРН 34.** Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та кібербезпеки відповідно до цілей і завдань організації.<br>**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.<br>**ПРН 36.** Виявляти небезпечні сигнали технічних засобів<br>**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.<br>**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.<br>**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.<br>**ПРН 40.** Забезпечувати неперервність процесу ведення |

| | |
|---|---|
| | журналів реєстрації подій та інцидентів на основі автоматизованих процедур.<br>**ПРН 41.** Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та кібербезпеки.<br>**ПРН 42.** Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.<br>**ПРН 43.** Вирішувати задачі забезпечення неперервності бізнес процесів організації на основі встановленої системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів.<br>**ПРН 44.** Застосовувати різні класи політик інформаційної безпеки та кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.<br>**ПРН 45.** Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.<br>**ПРН 46.** Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.<br>**ПРН 47.** Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.<br>**ПРН 48.** Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.<br>**ПРН 49.** Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).<br>**ПРН 50.** Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.<br>**ПРН 51.** Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.<br>**ПРН 52.** Вирішувати задачі аналізу програмного коду на наявність можливих загроз.<br>**ПРН 53.** Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність |

| | |
|---|---|
| | його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. |
| **8 – Ресурсне забезпечення реалізації програми** | |
| **Кадрове забезпечення** | Група забезпечення спеціальності 125 Кібербезпека сформована з числа науково-педагогічних працівників Навчально-наукового інституту захисту інформації Державного університету телекомунікацій. Кількісний та якісний склад групи відповідає ліцензійним вимогам. |
| **Матеріально-технічне забезпечення** | Теоретичні заняття проводяться в сучасних комп'ютерних класах та спеціалізованих лабораторіях, які оснащені спеціалізованими апаратно-програмними засобами.<br>Для проведення практичних та лабораторних занять з метою формування професійних компетенцій зі спеціальності 125 Кібербезпека використовуються 6 спеціалізованих лабораторій: «Інформаційної та кібербезпеки», «Кіберполігон», «Безпеки інформаційно-комунікаційних систем», «Систем технічного захисту інформації та автоматизації обробки», «Захисту інформації» та «Управління кібербезпекою».<br>Окрім оснащення сучасними комп'ютерами, програмно-апаратними комплексами та мультимедійними системами ці спеціалізовані лабораторії обладнані:<br>***лабораторія «Управління кібербезпекою»*** − програмними засобами підтримки прийняття рішень у сфері інформаційної безпеки («Вибір», MPRIORITY 1.0), програмами виявлення загроз інформаційній безпеці у режимі реального часу (IBM Security QRadar SIEM), засобами захисту від експлойтів (HitmanPro.Alert) та попутних завантажень (Cryptolocker), системою управління інформаційними ризиками і політикою безпеки (Digital Security), системами управління інформаційною безпекою («Гриф», «Кондор»), засобами аудиту безпеки мережевих пристроїв Titania Nipper Studio, пакетом Ethernet-перехоплення (Capsa Free), програмним комплексом моніторингу завдань інформаційної безпеки Ризик Менеджер-Інфо 4.3.2;<br>***лабораторія «Інформаційної та кібербезпеки»*** − міжмережевим екраном D-Link NetDefend, засобами проведення пентестингу (Pwn Pad, CreepyDOL, Demyo Power Strip), антивірусними програмами ESET Secure Business, мережевим обладнанням, таке як |

| | |
|---|---|
| | маршрутизатор Huawei та TP–Link, керованим комутатором та накопичувачем My Cloud Home, програмним забезпеченням Cicsco Packet Tracer GNC 3;<br>***лабораторія «Кіберполігон»*** **–** системою управління подіями та інцидентами кібербезпеки IBM Security QRadar SIEM, сканером уразливостей додатків IBM Security AppScan, системою запобігання вторгнень IBM Security Network Intrusion Prevention System.<br>***лабораторія «Безпеки інформаційно-комунікаційних систем»*** **–** програмним забезпеченням CrypTool, програмно-технічним комплексом «Центр сертифікації ключів», засобами криптографічного захисту IP-шифратор CryptoIP-448, електронним ключем "SecureToken-337, програмним IP-шифратором «CryptoIP-VPN Client», безконтактним карт-рідером КР-382, USB;<br>***лабораторія «Систем технічного захисту інформації та автоматизації обробки»*** **–** програмними комплексами моделювання (Electronic Workbench, Matlab Simulink, LabVIEW), зразками закладних пристроїв, обладнанням для пошуку засобів прихованого зняття інформації (DigiScan EX, «Піранья», AR 8200, IC-R2500, NR-900EM), програмними комплексами захисту інформації («Лоза», «Гриф», «Рубіж»);<br>***лабораторія «Захисту інформації»*** **–** автоматизованим комплексом відеоспостереження та охорони об'єктів інформаційної діяльності (Harbor), програмно-апаратними комплексами контролю доступу (HikVision), сповіщувачами інфрачервоними (SRP 600) та магніто-контактними (СОМК-10), генераторами акустичних та електромагнітних шумів (Ріас-2ГС, ГШ 1000, «Беркут»). |
| **Інформаційне та навчально-методичне забезпечення** | Всі дисципліни навчального плану забезпечені інформаційними та навчально-методичними матеріалами, засобами системи дистанційного навчання Moodle у т.ч. доступом до електронної бібліотеки Державного університету телекомунікацій. |
| **9 – Академічна мобільність** | |
| **Національна кредитна мобільність** | Наявність двосторонніх договорів між Державного університету телекомунікацій та закладами вищої освіти України забезпечує національну кредитну мобільність |
| **Міжнародна кредитна мобільність** | Зміст освітньої програми відповідає стандартам вищої освіти, що дозволяє приймати участь у програмах |

| | |
|---|---|
| | подвійних дипломів та бути конкурентоспроможним на світовому ринку праці |
| **Навчання іноземних здобувачів вищої освіти** | Передбачає навчання іноземців та осіб без громадянства |

## 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** | | | | |
| 1. | Групова динаміка і комунікації | ЗК12.1.01 | ЗК1, ЗК6 | ПРН3, ПРН6, ПРН53 |
| 2. | Ділові комунікації (Українська мова за професійним спрямуванням) | 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 інформаційної 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. | Застосування інформаційно-телекомунікаційних засобів | 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. | Фізичні поля як носії інформації | 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. | Апаратні та програмні засоби комп'ютерної інженерії | ПП12.2.03 | ЗК2, ПП2, | ПРН5, ПРН24, ПРН31 |
| 4. | Операційні системи | ПП12.2.04 | ЗК1, ПП2, | ПРН5, ПРН24, ПРН31, ПРН40 |
| 5. | Комп'ютерні мережі | ПП12.2.05 | ЗК2, ЗК5, ПП2, ПП11 | ПРН5, ПРН15, ПРН17, ПРН31 |
| 6. | Стандарти інформаційної та кібербезпеки | ПП12.2.06 | ЗК1, ЗК3, ЗК5, ПП1, | ПРН1, ПРН7, ПРН8 |
| 7. | Прикладна криптологія | ПП12.2.07 | ЗК2, ЗК7, ПП10 | ПРН31, ПРН46, ПРН47 |
| 8. | Аудит систем захисту інформації | ПП12.2.08 | ЗК1, ЗК4, ЗК5, ПП5, | ПРН4, ПРН9, ПРН11, ПРН18, ПРН41, ПРН45, ПРН49, ПРН52, |
| 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. | Штучний інтелект | ПП12.2.11 | ЗК2, ЗК5, ПП2, | ПРН5, ПРН17 |
| 12. | Компонентна база в системах захисту інформації | ПП12.2.12 | ЗК1, ЗК2, ПП3, ПП10 | ПРН15, ПРН36, ПРН37, ПРН38 |
| 13. | Поля і хвилі в системах технічного захисту інформації | ПП12.2.13 | ЗК1, ЗК2, ПП7, ПП10 | ПРН36, ПРН37, ПРН38 |
| 14. | Засоби передачі в системах технічного захисту інформації | ПП12.2.14 | ЗК1, ЗК2, ПП7, ПП10 | ПРН15, ПРН17, ПРН36, ПРН37, ПРН38 |
| 15. | Засоби прийому та обробки сигналів в системах технічного захисту інформації | ПП12.2.15 | ЗК1, ЗК2, ПП7, ПП10 | ПРН15, ПРН17, ПРН36, ПРН37, ПРН38 |
| 16. | Методи та засоби технічного захисту інформації | ПП12.2.16 | ЗК1, ЗК2, ПП3, ПП5, ПП7, ПП10, ПП12 | ПРН12, ПРН15, ПРН16, ПРН17, ПРН21, ПРН22, ПРН23, ПРН28, ПРН29, ПРН30, ПРН31, ПРН35, ПРН40 |
| 17. | Схемотехніка пристроїв технічного захисту інформації | ПП12.2.17 | ЗК1, ЗК2, ПП10, ПП12 | ПРН15, ПРН17, ПРН36, ПРН37, ПРН38 |

| | | | | |
|---|---|---|---|---|
| 18. | Безпека безпроводових, мобільних та хмарних технологій | 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 ІБ | ПП12.2.19 | ЗК1, ЗК2, ПП10, ПП12 | ПРН17, ПРН19, ПРН28, ПРН29, ПРН37 |
| 20. | Технічні засоби охорони обєктів | ПП12.2.20 | ЗК1, ЗК2, ПП10, ПП12 | ПРН23, ПРН28, ПРН29, ПРН30, ПРН31, ПРН35, ПРН40 |
| 21. | Менеджмент інформаційної безпеки | ПП12.2.21 | ЗК2, ПП2, | ПРН33 |
| 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** | | | | |
| **3.1. Дисципліни циклу загальної підготовки** | | | | |
| 1. | Іноземна мова* | ППк 12.3.01.01 | ЗК3 | ПРН1 |
| 2. | Іноземна мова професійного спрямування* | ППк 12.3.01.02 | ЗК2, ЗК3 | ПРН1, ПРН2 |
| **3.2. Дисципліни циклу професійної та практичної підготовки** | | | | |
| 3. | Захист від шкідливого програмного засобу | ППк 12.3.2.01 | ЗК1, ЗК4, ПП5, ПП6, ПП9 | ПРН5, ПРН14, ПРН18, ПРН20, ПРН49, ПРН51, ПРН52 |

| | | | | |
|---|---|---|---|---|
| 4. | *Інженерна та комп'ютерна графіка* | ППк 12.3.2.02 | ЗК2, ПП2, | ПРН10 |
| 5. | Аналіз та оцінка уразливостей інформаційних систем | ППк 12.3.2.03 | ЗК1, ЗК4, ЗК5, ПП8, ПП11, ПП12 | ПРН3, ПРН9, ПРН18, ПРН28, ПРН51 |
| 6. | *Перспективні компоненти та засоби інфокомунікаційних технологій* | ППк 12.3.2.04 | ЗК2, ПП2, | ПРН10 |
| 7. | Програмні комплекси захисту автоматизованих систем від несанкціонованого доступу | ППк 12.3.2.05 | ЗК2, ЗК4, ПП3, ПП7, ПП9 | ПРН7, ПРН 14, ПРН16, ПРН18, ПРН21, ПРН24, ПРН26, ПРН30, ПРН 50 |
| 8. | *Сучасні комп'ютерні системи та мережі* | ППк 12.3.2.06 | ЗК2 ПП2, | ПРН17, ПРН10, ПРН11, ПРН13, ПРН15 |
| 9. | Проектування систем технічного захисту інформації | ППк 12.3.2.07 | ЗК1, ЗК3, ЗК4, ЗК5, ПП3, ПП5, ПП7, ПП10, ПП12 | ПРН16, ПРН19, ПРН21, ПРН23, ПРН29, ПРН35, ПРН37, ПРН44 |
| 10. | *Системи управління електронним документообігом* | ППк 12.3.2.08 | ЗК1, ПП2, | ПРН10 |
| 11. | Кібербезпека банківських та комерційних структур | ППк 12.3.2.09 | ЗК1, ЗК4, ЗК5, ЗК7, ПП1, ПП4, ПП5, ПП6, ПП7, ПП8 | ПРН15, ПРН17, ПРН21, ПРН24, ПРН28, ПРН 32, ПРН34, ПРН41, ПРН42, ПРН44, ПРН48 |
| 12. | *Комп'ютерні технології вимірювань в телекомунікаціях* | ППк 12.3.2.10 | ЗК1, ПП2, | ПРН10, ПРН13 |
| 13. | Цифрова криміналістика | ППк 12.3.2.11 | ЗК1, ЗК2, ЗК5, ЗК7, ПП1, ПП6, ПП8, ПП11, ПП12 | ПРН15, ПРН21, ПРН 23, ПРН24, ПРН28, ПРН34, ПРН41, ПРН42, ПРН45 |
| 14. | *Інформаційні ресурси та сервіси в інфокомунікаціях* | ППк 12.3.2.12 | ЗК2, ПП2, | ПРН10, ПРН13, ПРН15 |
| 15. | Фізичні принципи передачі та прийому інформації в кіберпросторі | ППк 12.3.2.13 | ЗК1, ЗК2, ЗК3, ЗК5, ПП2, ПП5, ПП8 | ПРН1, ПРН4,ПРН14, ПРН17 |
| 16. | *Іноземна мова професійного спрямування (для дисципліни ППк 12.3.2.13)* | ППк 12.3.2.14 | ЗК1, ЗК2, ЗК3, ЗК5, ПП2, ПП5, ПП8 | ПРН1, ПРН4,ПРН14, ПРН17 |

| | | | | |
|---|---|---|---|---|
| 17. | Стандартизація технічних систем захисту інформації та правові основи контролю інформаційною безпекою | ППк 12.3.2.15 | ЗК2, ЗК3, ЗК4, ПП1, ПП3, ПП4, ПП5, ПП6 | ПРН1, ПРН2,ПРН7, ПРН16 |
| 18. | *Іноземна мова професійного спрямування (для дисципліни ППк 12.3.2.14)* | ППк 12.3.2.16 | ЗК2, ЗК3, ЗК4, ПП1, ПП3, ПП4, ПП5, ПП6 | ПРН1, ПРН2,ПРН7, ПРН16 |
| 19. | Експлуатація технічних систем захисту інформації | ППк 12.3.2.17 | ЗК1, ЗК2, ЗК3, ЗК5, ПП2, ПП4, ПП5, ПП8 | ПРН1, ПРН4,ПРН14, ПРН18, ПРН25 |
| 20. | *Іноземна мова професійного спрямування (для дисципліни ППк 12.3.2.15)* | ППк 12.3.2.18 | ЗК1, ЗК2, ЗК3, ЗК5, ПП2, ПП4, ПП5, ПП8 | ПРН1, ПРН4,ПРН14, ПРН18, ПРН25 |

* 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 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 |
| 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 | 3 | Іспит |

| | | | |
|---|---|---|---|
| | інформації | | |
| 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 об’єктів | 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 | | Залік, Іспит |
| *Вибірковий блок 2 (за вибором студентів)* | | | |
| ППк 12.3.2.01 | Захист від шкідливого програмного засобу | 5 | Залік |
| ППк 12.3.2.02 | *Інженерна та комп’ютерна графіка* | | |
| *Вибірковий блок 3 (за вибором студентів)* | | | |
| ППк 12.3.2.03 | Аналіз та оцінка уразливостей інформаційних систем | 5 | Іспит |
| ППк 12.3.2.04 | *Перспективні компоненти та засоби інфокомунікаційних технологій* | | |
| *Вибірковий блок 4 (за вибором студентів)* | | | |
| ППк 12.3.2.05 | Програмні комплекси захисту автоматизованих систем від несанкціонованого доступу | 5 | Іспит |
| ППк 12.3.2.06 | *Сучасні комп’ютерні системи та мережі* | | |
| *Вибірковий блок 5 (за вибором студентів)* | | | |
| ППк 12.3.2.07 | Проектування систем технічного захисту інформації | 5 | Іспит |
| ППк 12.3.2.08 | *Системи управління електронним документообігом* | | |
| *Вибірковий блок 6 (за вибором студентів)* | | | |
| ППк 12.3.2.09 | Кібербезпека банківських та комерційних структур | 5 | Іспит |
| ППк 12.3.2.10 | *Комп’ютерні технології вимірювань в телекомунікаціях* | | |
| *Вибірковий блок 7 (за вибором студентів)* | | | |
| ППк 12.3.2.11 | Цифрова криміналістика | 5 | Іспит |
| ППк 12.3.2.12 | *Інформаційні ресурси та сервіси в інфокомунікаціях* | | |
| *Вибірковий блок 8 (за вибором студентів)* | | | |
| ППк 12.3.2.13 | Фізичні принципи передачі та прийому інформації в кіберпросторі | 5 | Іспит |
| ППк 12.3.2.14 | *Іноземна мова професійного спрямування (для дисципліни ППк 12.3.2.13)* | | |
| *Вибірковий блок 9 (за вибором студентів)* | | | |
| ППк 12.3.2.15 | Стандартизація технічних систем захисту інформації та правові основи контролю інформаційної та кібербезпеки | 5 | Іспит |
| ППк 12.3.2.16 | *Іноземна мова професійного спрямування (для дисципліни ППк 12.3.2.15)* | | |
| *Вибірковий блок 10 (за вибором студентів)* | | | |

| | | | |
|---|---|---|---|
| ППк 12.3.2.17 | Експлуатація технічних систем захисту інформації | 10 | Іспит |
| ППк 12.3.2.18 | *Іноземна мова професійного спрямування (для дисципліни ППк 12.3.2.17)* | | |
| **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 та практичної 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*** | ***8*** | ***Всього*** | ***12*** | | |
| | ***Всього за I курс*** | ***30*** | | ***30*** | **60** | **25** |

| Цикл | 2 курс | | | | Всього | |
|---|---|---|---|---|---|---|
| | 3 семестр | | 4 семестр | | Кр. | % |
| Цикл загальної підготовки | Вища математика | 4 | Ділові комунікації (Українська мова за професійним спрямуванням) | 3 | | |
| | Теорія інформації та кодування | 4 | Філософія | 3 | | |
| | Фізичні поля як носії інформації | 3 | | | | |
| | ***Всього*** | ***11*** | ***Всього*** | ***6*** | | |
| Цикл професійної та практичної 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<br>*Іноземна мова професійного спрямування* | 5 | Іноземна мова<br>*Іноземна мова професійного спрямування* | 5 | | |
| | Захист від шкідливого програмного засобу | 5 | Аналіз та оцінка уразливостей інформаційних систем | 5 | | |
| | *Інженерна та комп'ютерна графіка* | | *Перспективні компоненти та засоби інфокомунікаційних технологій* | | | |
| | ***Всього*** | ***10*** | ***Всього*** | ***10*** | | |
| | ***Всього за 2 курс*** | ***30*** | | ***30*** | **60** | **25** |

| Цикл | 3 курс | | | | Всього | |
|---|---|---|---|---|---|---|
| | 5 семестр | | 6 семестр | | Кр. | % |
| Цикл професійної та практичної 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 | Фізичні принципи передачі та прийому інформації в кіберпросторі *(Іноземна мова професійного спрямування для дисципліни «Фізичні принципи передачі та прийому інформації в кіберпросторі»)* | 5 | Стандартизація технічних систем захисту інформації та правові основи контролю інформаційної та кібербезпеки (*Іноземна мова професійного спрямування для дисципліни «Стандартизація технічних систем захисту інформації та правові основи контролю інформаційної та кібербезпеки»)* | 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*** | ***30*** | | ***30*** | **60** | **25** |

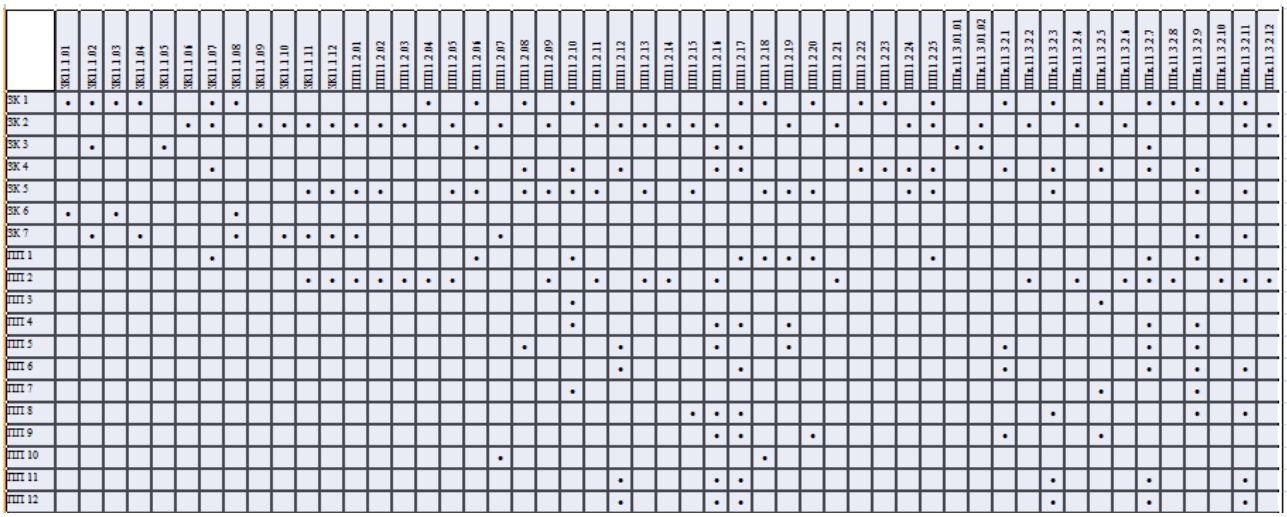
| Цикл | 4 курс | | | | Всього | |
|---|---|---|---|---|---|---|
| | 7 семестр | | 8 семестр | | Кр. | % |
| Цикл загальної підготовки | Засади відкриття власного бізнесу | 3 | | | | |
| | ***Всього*** | ***3*** | ***Всього*** | | | |
| Цикл професійної підготовки | Хмарні технології | 3 | Штучний інтелект | 3 | | |
| | Комплексні системи захисту інформації | 5 | Комплексні системи захисту інформації | 5 | | |
| | Технічні засоби охорони об'єктів | 3 | Переддипломна практика | 6 | | |
| | Метрологія та вимірювання в ІБ | 3 | Кваліфікаційна робота Підсумкова атестація | 6 | | |
| | Менеджмент інформаційної безпеки | 3 | | | | |
| | ***Всього*** | ***17*** | ***Всього*** | ***20*** | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Вільного вибору студента** | Експлуатація технічних систем захисту інформації *(Іноземна мова професійного спрямування для дисципліни «Експлуатація технічних систем захисту інформації»)* | 5 | Експлуатація технічних систем захисту інформації *(Іноземна мова професійного спрямування для дисципліни «Експлуатація технічних систем захисту інформації»)* | 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*** | ***30*** | | ***30*** | **60** | **25** |
| **Всього** | | **120** | | **120** | **240** | **100** |

## 3. Форма атестації здобувачів вищої освіти

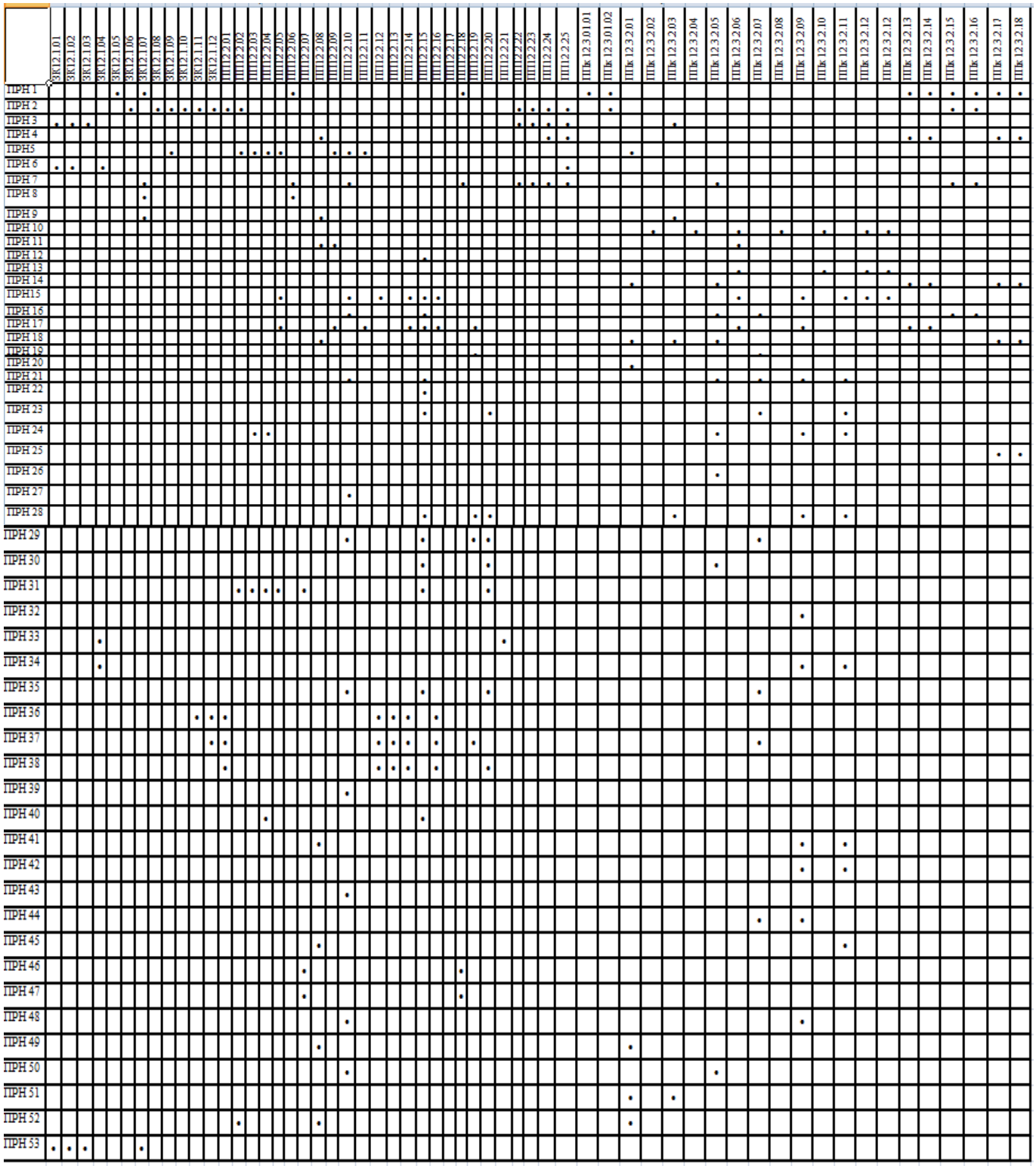
| | |
|---|---|
| **Форми атестації здобувачів вищої освіти** | Атестація здобувачів вищої освіти здійснюється у формі публічного захисту кваліфікаційної роботи. |
| **Вимоги до кваліфікаційної роботи** | Кваліфікаційна робота передбачає розв’язання спеціалізованої задачі в галузі інформаційної та кібернетичної безпеки. Має бути перевірена на плагіат відповідно до «Положення про запобігання академічному плагіату у Державному університеті телекомунікацій» та оприлюднено у репозитарії Університету. |

# 4. Матриця відповідності програмних компетентностей компонентам освітньої програми



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

.




**Гарант освітньої програми**

Завідувач кафедри систем інформаційного
та кібернетичного захисту Навчально-наукового інституту
захисту інформації, доктор технічних наук,
старший дослідник **В.А. Савченко**