МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

«КІБЕРБЕЗПЕКА МОБІЛЬНИХ ТА ВІДЕОІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ»

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

першого (бакалаврського) рівня вищої освіти

(ПРОЄКТ)

Галузь знань **F «Інформаційні технології»**
Спеціальність **F5 «Кібербезпека та захист інформації»**
Кваліфікація: **«Бакалавр з кібербезпеки мобільних та відеоінформаційних технологій»**

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ УНІВЕРСИТЕТУ

Протокол № ____ від _____ 2026 р.

Наказ № ____ від _____ 2026 р.

Ректор _____ Володимир ШУЛЬГА

Освітня програма вводиться в дію

з 01 вересня 2026 р.

Київ 2026

ЛИСТ ПОГОДЖЕННЯ
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«КІБЕРБЕЗПЕКА МОБІЛЬНИХ ТА ВІДЕОІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ»
ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

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

1. Перший проректор _____ Олександр КОРЧЕНКО

2. Проректор з навчальної роботи _____ Артур ГУДМАНЯН

3. Начальник навчально-методичного відділу _____ Вадим ВЛАСЕНКО

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

Голова вченої ради ННІКБЗІ _____ Євгенія ІВАНЧЕНКО

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

Завідувач кафедри технічних
систем кіберзахисту _____ Олександр ТУРОВСЬКИЙ

Голова студентської ради ННІКБЗІ _____ Станіслав ШТЕФАН

Рецензії від зовнішніх стейкхолдерів:

1. ТОВ «ЛУЧ»;
2. ТОВ «А.А.Г.».

ПЕРЕДМОВА

Розроблено робочою групою у складі:

Гарант освітньої програми (голова робочої групи):

Ігор ІВАНЧЕНКО – кандидат технічних наук, доцент, професор кафедри технічних систем кіберзахисту.

Члени робочої групи:

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

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

ВІДОМОСТІ ПРО ПЕРЕГЛЯД ОСВІТНЬОЇ ПРОГРАМИ

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

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

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

1. Профіль освітньої програми

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Державний університет інформаційно-комунікаційних технологій. Навчально-науковий інститут кібербезпеки та захисту інформації.
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр. Освітня кваліфікація – бакалавр з кібербезпеки мобільних та відеоінформаційних технологій.
Офіційна назва освітньої програми	Освітньо-професійна програма «Кібербезпека мобільних та відеоінформаційних технологій».
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний на базі повної загальної середньої освіти. Обсяг освітньої програми – 240 кредитів ЄКТС; Термін навчання 3 роки 10 місяців денної форми навчання на базі ступеня молодшого бакалавра (освітньо-кваліфікаційного рівня «молодшого спеціаліста») при перезарахуванні не більше 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки.
Наявність акредитації	Сертифікат про акредитацію спеціальності 125 Кібербезпека УД № 11009229 від 18.04.19 р. Термін дії сертифікату 01.07.2029 р.
Цикл/рівень	НРК України – 6 рівень/Бакалавр QF-EHEA – перший цикл EQF-LLL – 6 рівень
Передумови	Наявність атестата про повну загальну середню освіту або диплома молодшого бакалавра (освітньо-кваліфікаційного рівня «молодший спеціаліст»).
Мова(и) викладання	Українська, англійська.
Термін дії освітньої програми	Програма вводиться в дію з 01.09.2026 року. Програма дійсна впродовж дії державних стандартів вищої освіти та може бути відкоригована відповідно до діючих нормативних документів Університету.
Інтернет-адреса постійного розміщення опису освітньої програми	http://www.duikt.edu.ua/ua/1823-osvitno-profesiyni-programi-kafedra-technicnih-system-kiberzagistu

2 – Мета освітньої програми	
Метою бакалаврської програми є підготовка компетентних фахівців, здатних проектувати, впроваджувати та адмініструвати комплексні системи кібербезпеки з поглибленим фокусом на захисті мобільних платформ, додатків та відеоінформаційних технологій. Програма спрямована на формування здатності розв'язувати складні спеціалізовані задачі захисту мультимедійних даних, безпеки бездротових мереж та відеоспостереження, з правом подальшої професійної діяльності на підприємствах державного та комерційного сектору.	
3 – Характеристика освітньої програми	
Предметна область, Напрям (галузь знань, спеціальність)	**Об'єкти професійної діяльності випускників:** - об'єкти інформатизації, а саме: комп'ютерні, мобільні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні (включаючи системи відеомоніторингу та обробки відеоданих), інформаційно-комунікаційні системи та мережі (зокрема бездротові та стільникові), інформаційні ресурси та технології; - системи та технології забезпечення безпеки інформації, засоби технічного та криптографічного захисту мультимедійного контенту та мобільних додатків; - процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту, з урахуванням специфіки мобільного простору та відеоінформаційного середовища. **Теоретичний зміст предметної діяльності.** Знання: - законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності, зокрема у сфері телекомунікацій та захисту персональних даних; - принципів супроводу систем та комплексів кібербезпеки, архітектури безпеки мобільних операційних систем та платформ відеонагляду; - теорій, моделей та принципів управління доступом до інформаційних ресурсів, хмарних сховищ відеоданих та мобільних застосунків; - методів та засобів виявлення та ідентифікації каналів витоку інформації, в тому числі технічними каналами та через вразливості бездротових протоколів передачі даних;

	- методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах та мережах відеомоніторингу; - методів та засобів технічного та криптографічного захисту інформації, методів комп'ютерної стеганографії та захисту мультимедійного контенту. F «Інформаційні технології». F5 «Кібербезпека та захист інформації».
Орієнтація освітньої програми	Освітня. 100% обсягу освітньої програми спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю F5 «Кібербезпека та захист інформації» визначеного стандартом вищої освіти. Програма носить прикладний характер, спрямована на забезпечення потреб ринку праці.
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта та професійна підготовка в галузі кібербезпеки та захисту інформації з поглибленим вивченням мобільних та відеоінформаційних систем. Підготовка фахівців, здатних використовувати і впроваджувати спеціалізовані технології, методи та засоби захисту мультимедійного контенту, безпеки бездротових мереж, мобільних платформ та інфраструктури відеомоніторингу. **Ключові слова:** КІБЕРБЕЗПЕКА, МОБІЛЬНІ ТЕХНОЛОГІЇ, ВІДЕОІНФОРМАЦІЙНІ СИСТЕМИ, ЗАХИСТ МУЛЬТИМЕДІА, БЕЗПЕКА БЕЗДРОТОВИХ МЕРЕЖ, СТЕГАНОГРАФІЯ, ЗАХИСТ ІНФОРМАЦІЇ.
Опис предметної області	**Об’єкти професійної діяльності випускників**: - технології кібербезпеки та захисту інформації, зокрема технології захисту мобільних платформ, бездротових мереж та відеоінформаційних потоків; - процеси управління кібербезпекою та захистом інформації, безпекою мобільних додатків та систем відеоспостереження; - об'єкти інформаційної діяльності, в тому числі мобільні інформаційні та інформаційно-комунікаційні системи, системи обробки відеоданих, інформаційні ресурси мультимедійного характеру і технології. **Цілі навчання:** підготовка фахівців, здатних використовувати і впроваджувати методи і технології кібербезпеки в мобільних та

	мультимедійних системах, а також системи захисту відеоінформаційних ресурсів та розв'язувати складні задачі у галузі безпеки бездротових телекомунікацій та захисту інформації. **Теоретичний зміст предметної діяльності** Принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, мобільних комунікацій та відеоінформаційних систем; сучасні технології захисту, які забезпечують сталий розвиток інформаційного суспільства, безпеку мультимедійного контенту, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз інформації та національній безпеці України в бездротових мережах та системах відеомоніторингу. **Методи, методики та технології:** методи, методики, технології, способи розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації, зокрема методи аналізу захищеності мобільних додатків, технології захисту потокового відео, методи стеганографії та криптографічного захисту мультимедійних даних, а також методики виявлення вразливостей у бездротових інтерфейсах та протоколах. **Інструменти та обладнання:** засоби, пристрої, мережне устаткування (в т.ч. бездротове та комутаційне обладнання відеосистем), прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси (включаючи системи відеоспостереження та мобільні платформи) для проєктування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних та відеопотоків).
Особливості програми	Програма передбачає: - викладання окремих дисциплін циклу професійної підготовки англійською мовою (з поглибленим вивченням технічної термінології у сфері мобільних комунікацій та мультимедіа); - передбачено в межах навчального процесу отримання сертифікатів від провідних компаній в галузі телекомунікацій, розробки мобільних платформ та систем відеонагляду; - залучення до проведення практичних занять та лабораторних робіт фахівців-практиків з кібербезпеки, експертів із захисту мобільних мереж

	та інженерів систем відеомоніторингу; - забезпечення умов підготовки здобувачів вищої освіти у реальному середовищі до майбутньої професійної діяльності для набуття відповідних компетенцій, шляхом організації проведення практик (ознайомча, виробнича та переддипломна) в організаціях-партнерах з можливістю подальшого працевлаштування.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Бакалавр з кібербезпеки мобільних та відеоінформаційних за освітньою програмою «Технічні системи кіберзахисту» (випускник) здатний виконувати професійні роботи за Державним класифікатором професій ДК 003:2010: - фахівець з технічного захисту інформації, 2139.2; - аналітик з безпеки інформаційно-телекомунікаційних систем, 2139.2 - аудитор інформаційних технологій (з кібербезпеки), 2139.2 - адміністратор безпеки мереж і систем, 2139.2; - фахівець сфери захисту інформації, 2139.2; - фахівець з питань безпеки (інформаційно-комунікаційні технології), 2139.2; - конструктор систем кібербезпеки, 2132.2; - фахівець з підтримки інфраструктури кіберзахисту, 2139.2; - фахівець з реагування на інциденти кібербезпеки, 2139.2; - фахівець з криптографічного захисту інформації, 2139.2; - фахівець з тестування систем захисту інформації, 2139.2; - фахівець з оцінки заходів захисту інформації (кібербезпеки), 2139.2 та міжнародної стандартної класифікації професій International Standard Classification of Occupation 2008: 2529 Security specialist (ICT) – Спеціаліст з безпеки (інформаційно-комунікаційні технології), 3512 Information and communications technology user support technicians – Технічні фахівці служби підтримки користувачів ІКТ (актуально для підтримки мобільних корпоративних мереж). Існує можливість отримати міжнародні сертифікати в галузі кібербезпеки та мережевих технологій (наприклад, CompTIA Security+, Cisco Certified

	CyberOps Associate, Certified Mobile Security Professional).
Подальше навчання	Можливість продовжити навчання за освітньою програмою другого (магістерського) освітнього рівня вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Проблемно-орієнтоване навчання. Викладання проводиться державною та іноземною (викладання окремих дисциплін проводиться англійською) мовами, які формують професійні компетенції. Викладання спрямовано на засвоєння знань, умінь і навичок для подальшого застосування у практиці. Основними способами передачі змісту освітньої програми є проведення лекцій, семінарських, практичних, індивідуальних, лабораторних занять, консультації, розв'язання ситуаційних задач, тестування, презентації, ознайомча, виробнича, переддипломна практики.
Оцінювання	Оцінювання сформованих компетенцій під час контрольних заходів, які передбачені цією освітньою програмою зазначені у навчальному плані. Критерії оцінювання знань, умінь та навичок розроблені у відповідності до чинного законодавства та висвітлено у Положенні про організацію освітнього процесу у Державному університеті інформаційно-комунікаційних технологій.
6 – Програмні компетенції	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації, зокрема у сфері функціонування мобільних та відеоінформаційних технологій, що передбачає застосування теорій та методів захисту інформації і характеризується комплексністю та невизначеністю умов.
Загальні компетентності (ЗК)	**ЗК1**. Здатність застосовувати знання у практичних ситуаціях. **ЗК2**. Знання та розуміння предметної області та розуміння професії. **ЗК3**. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. **ЗК4**. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

	ЗК5. Здатність до пошуку, оброблення та аналізу інформації. **ЗК6**. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного)суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина і Україні. **ЗК7**. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. ЗК8. Здатність до абстрактного мислення, аналізу та синтезу.
Спеціальності (фахові предметні компетентності)	**СК1**. Здатність застосовувати законодавчу та нормативно- правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності, зокрема стандарти захисту персональних даних у системах відеонагляду та телекомунікаціях. **СК2**. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації для забезпечення надійності мобільних платформ та відеоінформаційних ресурсів. **СК3**. Здатність забезпечувати неперервність бізнес-процесів та безперебійну роботу систем відеомоніторингу згідно встановленої політики кібербезпеки та захисту інформації. **СК4**. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. **СК5**. Здатність відновлювати функціонування Інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. **СК6**. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів, включаючи системи контролю доступу та відеоаналітики).

	СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою з урахуванням особливостей мобільного середовища. **СК8**. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. **СК9**. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності для запобігання витоку інформації технічними каналами та побічними електромагнітними випромінюваннями. **СК10**. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам, включаючи аналіз відеопотоків та сигналів мобільних мереж, згідно з встановленою політикою інформаційної безпеки. **СК11**. Здатність розробляти та тестувати захищене програмне забезпечення для мобільних пристроїв, виявляти вразливості в коді мобільних додатків та операційних систем. **СК12**. Здатність застосовувати технології стеганографії та стеганоаналізу для захисту авторських прав та перевірки достовірності відеоінформації.
7 – Програмні результати навчання	
Результати навчання (РН)	**РН1**. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. **РН2**. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. **РН3**. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. **РН4**. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. **РН5**. Оцінювати, інтерпретувати, аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті

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

	відновлення інформації. **РН15**. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи. **РН16**. Вирішувати задачі впровадження та супроводу комплексних інформаційних системах. **РН17**. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. **РН18**. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. **РН19**. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів щодо захищеності мобільного зв'язку. **РН20**. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. **РН21**. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей мобільних додатків, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації інформаційних системах.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Група забезпечення спеціальності F5 Кібербезпека та захист інформації сформована із числа науково-педагогічних працівників Навчально-наукового інституту кібербезпеки та захисту інформації. Кількісний та якісний склад групи відповідають ліцензійним вимогам.

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

	інформації в інформаційно-комунікаційних системах, віртуальних приватних мереж VPN, електронного цифрового підпису та інфраструктури відкритих ключів. Спеціалізований програмно-апаратний комплекс ESET Protect дозволяє відпрацьовувати навички для захисту кінцевих точок. НАВЧАЛЬНА ЛАБОРАТОРІЯ «Мережевої безпеки». Лабораторія призначена для вивчення технологій мережевої безпеки CISCO та HUAWEI з можливістю проходження сертифікаційних курсів. НАВЧАЛЬНА ЛАБОРАТОРІЯ «Security Operation Center». Лабораторія призначена для проведення занять з питань аналізу, обробки та аудиту інформаційної безпеки. Крім того, дозволяє вивчати методи управління ризиками на основі методологій CRAMM, OCTAVE та RiskWatch у відповідності до вимог міжнародних стандартів з кібербезпеки та захисту інформації. Стенд «Систем безпеки та телекомунікаційного обладнання із штучним інтелектом» Відеокамера Hikvision DS-2CD2143G2-LIS2U. Відеокамера Hikvision DS-2CD2347G2H-LIU eF. Відеокамера цифрова Hikvision DS-2CD2443G2-I. Відеореєстратор DS-7604NXI-K1(B). Жорсткий диск WD10PURU-78. POE комутатор DS-3T1310P-SI/HS. IP відеодомофон DS-KH6110-WE1. Викликова панель відеодомофону DS-KV6113-WPE1(C). Панель-контроллер доступу DS-K1T321MX. Комплект управління безпекою DS-PWA64-Kit-WE. Кронштейн DS-1294ZJ-TRL. Комутатор DS-3E0505D-E. Відеокамера цифрова PanoVU PTZ Hikvision DS-2PT31221Z-DE3. Кабель КПВ-ВП (350) 4*2*0,51 (U/UTP-cat.SE), 100м. Короб пластиковий e.trunking.stand.60.40, 60х40мм, 2м ЕНЕКСТ. Конектор RJ45 кат. 5е, неекранований ((Упаковка 100 Шт). Дослідження сучасних систем відеоспостереження на основі IP-технологій. Вивчення основних вимог до систем IP-відеоспостереження та вибір устаткування для проектування. Для проведення практичних та лабораторних занять

	також використовуються: - Network FishEye Camera; - Вулична циліндрична P-камера; - Indoor Box Network IP-камера; - IR CUBE Network Camera; - IR MINI BULLET Network Camera; - Network Video Recorder; - Комутатор Utepo. **Навчально-тренінговий центр відеотехнологій Axis, Milestone, Vezha.** Ця лабораторія створена як сучасний навчально-тренінговий простір, де студенти мають змогу здобути практичні навички роботи з найсучаснішими системами IP-відеоспостереження. 1. Проведення практичних занять із налаштування інтелектуальних систем відеоспостереження на основі IP-технологій. 2. Формування у студентів компетенцій проєктування, впровадження обслуговування систем IP-відеоспостереження. 3. Організація сертифікаційних курсів, з а результатами яких студенти отримують офіційні сертифікати партнерів. **Використання програмного забезпечення:** - MATLAB 2023 - пакет прикладних програм для вирішення завдань технічних обчислень, а також мова програмування; - Cisco Packet Tracer - це багатофункціональнапрограма моделювання мереж, яка дозволяє експериментувати з поведінкою мережі і оцінювати можливі сценарії. - GNU Octave - система для виконання математичних розрахунків, що надає інтерпретовану мову, багато в чому сумісну 3 Matlab. GNU Octave може використовуватися для розв'язування лінійних, нелінійних та диференціальних рівнянь, обчислень з використанням комплексних чисел і матриць, візуалізації даних, експериментів. - Multisim – програмне забезпечення промислового стандарта, яке підтримує більше 2000 SPICE-моделей компонентів для моделювання і програмування схем аналогової і цифрової електроніки. - IP Video System Design Tool 2024 - інструмент для планування, проектування та аналізу ефективності систем відеоспостереження.

Інформаційне та навчально-методичне забезпечення	Інформація про освітню програму, її освітні компоненти та вимоги до осіб, які можуть здобувати вищу освіту за цією програмою розміщена на офіційному сайті Державного університету інформаційно-комунікаційних технологій. Усі освітні компоненти освітньої програми забезпечені навчально-методичними матеріалами, є у вільному доступі у якості ресурсів бібліотеки, системи дистанційного навчання (GWE) університету.
9 – Академічна мобільність	
Національна кредитна мобільність	Наявність двосторонніх договорів між Державним університетом інформаційно-комунікаційних технологій та закладами вищої освіти України забезпечує національну кредитну мобільність.
Міжнародна кредитна мобільність	Зміст навчання відповідає світовим освітнім стандартам, що дозволяє приймати участь у програмах подвійних дипломів та бути конкурентоспроможним на світовому ринку праці.
Навчання іноземних здобувачів вищої освіти	_

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

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

№ з.п.	Дисципліна	Шифр	Компетентність	Результат навчання
1. Цикл дисциплін загальної підготовки				
1.	Теоретична підготовка базової загальновійськової підготовки	ОК1	ЗК3, ЗК6	РН1,РН3
2.	Групова динаміка і комунікації	ОК2	ЗК1, ЗК6	РН2, РН6
3.	Ділові комунікації (Українська мова професійного спрямування)	ОК3	ЗК1, ЗК3, ЗК7	РН2
4.	Філософія	ОК4	ЗК1, ЗК6	РН1, РН16
5.	Засади відкриття власного бізнесу	ОК5	ЗК1, ЗК7	РН4, РН11
6.	Іноземна мова *	ОК6	ЗК3	РН2
7.	Вища математика	ОК7	ЗК2	РН8
8.	Нормативно-правове забезпечення та міжнародні стандарти інформаційної та кібернетичної безпеки	ОК8	ЗК2, ЗК3, ЗК5, СК1	РН9
9.	Соціально-екологічна безпека життєдіяльності	ОК9	ЗК1 ЗК6, ЗК7	РН1
10.	Інформаційно-комунікаційні системи	ОК10	ЗК2, СК2	РН10, РН12
11.	Фізика	ОК11	ЗК2, ЗК7	РН8, РН20
12.	Теорія інформації та кодування	ОК12	ЗК2, ЗК5, ЗК7, СК2	РН7
13.	Менеджмент інформаційної безпеки	ОК13	ЗК2, ЗК5, ЗК7, СК2	РН9, РН11, РН17
2. Цикл дисциплін професійної та практичної підготовки				
1.	Безпека та захист систем мобільного зв’язку (4G/5G/6G)	ОК14	ЗК4, СК4, СК9	РН5, РН8, РН11
2.	Кібермоніторинг і аналіз стану телекомунікаційних мереж	ОК15	ЗК4, СК5, СК10	РН15, РН17, РН21

3.	Інтелектуальні системи відеоаналітики та кіберзахисту	ОК16	ЗК2, ЗК5, СК1, СК6, СК12	РН7, РН13, РН18
4.	Теорія кіл і сигналів в інформаційному та кіберпросторах	ОК17	ЗК2, ЗК5, ЗК7, СК2	РН7, РН8
5.	Прикладне програмування	ОК18	ЗК2, ЗК5, СК2	РН10, РН18
6.	Проектування систем безпеки об'єктів критичної інфраструктури	ОК19	ЗК2, СК2	РН3, РН9, РН13
7.	Операційні системи	ОК20	ЗК1, СК2	РН10, РН12
8.	Аналіз та оцінка уразливостей інформаційних систем	ОК21	ЗК2, ЗК5, ОК2, СК11	РН14, РН21
9.	Захист від шкідливого програмного засобу	ОК22	ЗК1, ЗК3, ЗК5, СК1	РН15, РН21
10.	Прикладна криптологія	ОК23	ЗК2, ЗК7, СК10	РН1, РН12
11.	Система менеджменту інформаційної безпеки	ОК24	ЗК1, ЗК4, ЗК5, СК5, СК6, СК9	РН9, РН11, РН12, РН17
12.	Хмарні технології	ОК25	ЗК2, ЗК5, ОК2, СК11	РН3, РН12
13.	Комплексні системи захисту інформації	ОК26	ЗК1, ЗК4, ЗК5, СК1, СК3, СК7	РН3, РН9, РН13
14.	Системи штучного інтелекту в кібербезпеці	ОК27	ЗК2, ЗК5, СК2, СК11	РН6, РН18
15.	Поля і хвилі в системах технічного захисту інформації	ОК28	ЗК2, ЗК5, СК11	РН8, РН20
16.	Засоби передачі в системах технічного захисту інформації	ОК29	ЗК2, ЗК4, СК3, СК7, СК9	РН7, РН 20
17.	Засоби прийому та обробки сигналів в системах технічного захисту інформації	ОК30	ЗК2, ЗК5, СК8	РН7, РН20
18.	Методи та засоби технічного захисту інформації	ОК31	ЗК1, ЗК3, ЗК4, СК1, СК4, СК6, СК8, СК9, СК11, СК12	РН9, РН20
19.	Схемотехніка пристроїв технічного захисту інформації	ОК32	ЗК1, ЗК3, ЗК4, ЗК5, СК1, СК2, СК4, СК5, СК6, СК11, СК12	РН13, РН20
20.	Метрологія та вимірювання в інформаційній безпеці	ОК33	ЗК2, ЗК5, СК1, СК4, СК5	РН2, РН20
21.	Цифрова криміналістика	ОК34	ЗК1, ЗК2, ЗК5, ЗК7, СК1, СК6, СК8, СК10, СК11,	РН15, РН9

			СК12	
22.	Ознайомча практика	ОК35	ЗК1, ЗК4	РН4
23.	Виробнича практика	ОК36	ЗК1, ЗК4	РН1, РН5, РН13, РН17
24.	Переддипломна практика	ОК37	ЗК2, ЗК4, ЗК5	РН3, РН14, РН15
25.	Кваліфікаційна робота	ОК38	ЗК1, ЗК2, ЗК4, ЗК5, СК1	РН3, РН5, РН16, РН9
26.	Підсумкова атестація			
3. Дисципліни вільного вибору студента				
1.	Дисципліна вільного вибору студента			
2.	Дисципліна вільного вибору студента			
3.	Дисципліна вільного вибору студента			
4.	Дисципліна вільного вибору студента			
5.	Дисципліна вільного вибору студента			
6.	Дисципліна вільного вибору студента			
7.	Дисципліна вільного вибору студента			
8.	Дисципліна вільного вибору студента			
9.	Дисципліна вільного вибору студента			

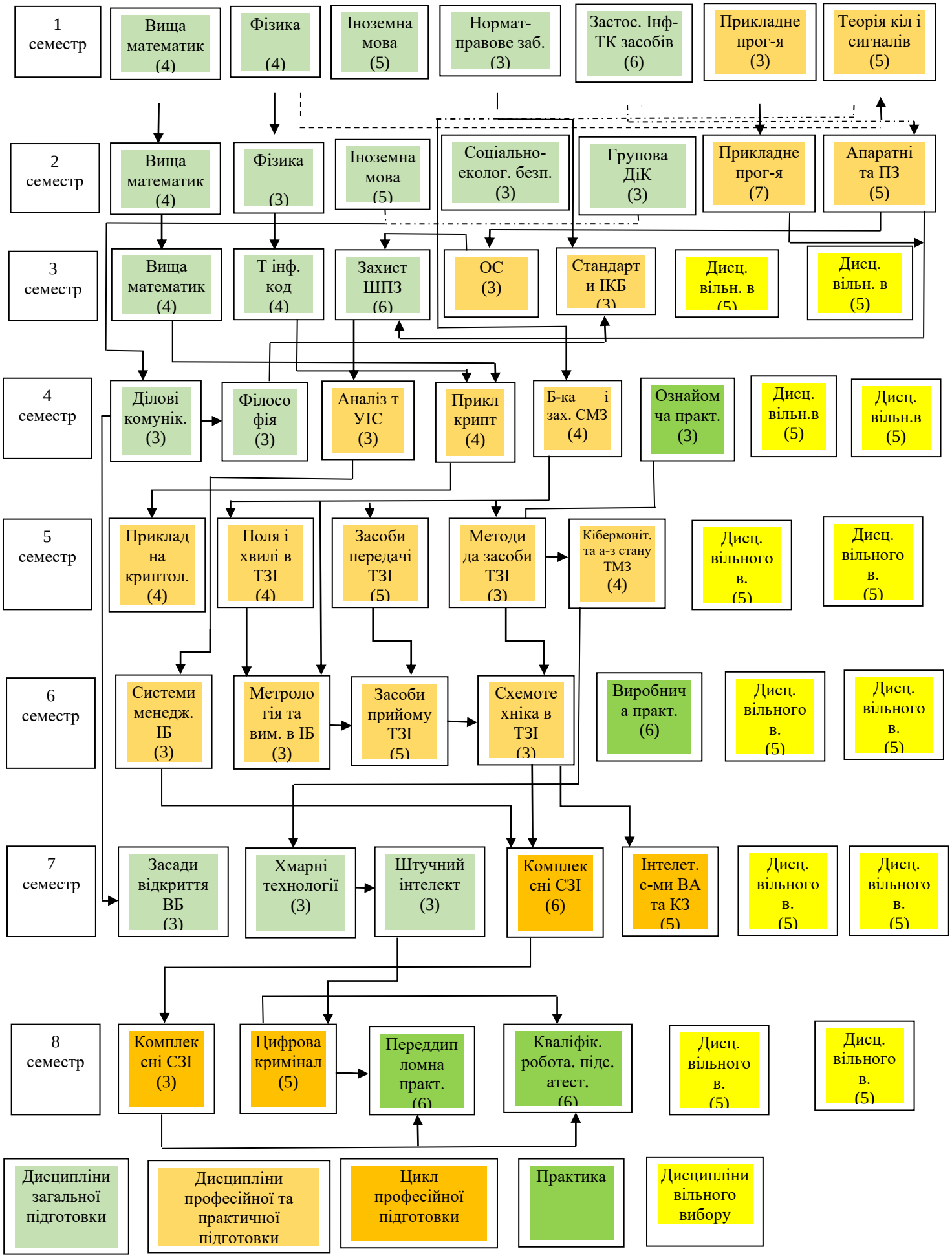
* Іноземна мова у навчальних планах для іноземців та осіб без громадянства замінюється на українську мову (за професійним спрямуванням).

2.2. Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
Обов'язкові компоненти ОП			
ОК1	Теоретична підготовка базової загальновійськової підготовки	3	Залік
ОК2	Групова динаміка і комунікації	3	Залік
ОК3	Ділові комунікації (Українська мова за професійним спрямуванням)	3	Залік
ОК4	Філософія	3	Іспит
ОК5	Засади відкриття власного бізнесу	3	Залік
ОК6	Іноземна мова	10	Залік, Іспит
ОК7	Вища математика	12	Залік, Іспит
ОК8	Нормативно-правове забезпечення та міжнародні стандарти інформаційної та кібернетичної безпеки	3	Іспит
ОК9	Соціально-екологічна безпека життєдіяльності	3	Іспит
ОК10	Інформаційно-комунікаційні системи	6	Залік
ОК11	Фізика	7	Залік, Іспит
ОК12	Теорія інформації та кодування	4	Іспит
ОК13	Менеджмент інформаційної безпеки	3	Іспит
ОК14	Безпека та захист систем мобільного зв'язку (4G/5G/6G)	4	Залік
ОК15	Кібермоніторинг і аналіз стану телекомунікаційних мереж	4	Іспит
ОК16	Інтелектуальні системи відеоаналітики та кіберзахисту	5	Залік
ОК17	Теорія кіл і сигналів в інформаційному та кіберпросторах	5	Іспит, КР
ОК18	Прикладне програмування	10	Залік, Іспит
ОК19	Проектування систем безпеки об'єктів критичної інфраструктури	5	Залік
ОК20	Операційні системи	3	Іспит
ОК21	Аналіз та оцінка уразливостей інформаційних систем	3	Іспит
ОК22	Захист від шкідливого програмного засобу	6	Іспит
ОК23	Прикладна криптологія	8	Залік, Іспит
ОК24	Система менеджменту інформаційної безпеки	3	Залік
ОК25	Мікропроцесорні системи	3	Залік
ОК26	Комплексні системи захисту інформації	9	Залік, Іспит
ОК27	Системи штучного інтелекту в кібербезпеці	3	Залік
ОК28	Поля і хвилі в системах технічного захисту інформації	4	Залік, Іспит, КП
ОК29	Засоби передачі в системах технічного захисту інформації	5	Залік
ОК30	Засоби прийому та обробки сигналів в системах технічного захисту інформації	5	Залік

ОК31	Методи та засоби технічного захисту інформації	3	Залік
ОК32	Схемотехніка пристроїв технічного захисту інформації	3	Іспит
ОК33	Метрологія та вимірювання в інформаційній безпеці	3	Іспит
ОК34	Цифрова криміналістика	5	Іспит
ОК35	Ознайомча практика	3	Залік
ОК36	Виробнича практика	6	Залік
ОК37	Переддипломна практика	6	Залік
ОК38	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 здобувачів вищої освіти здійснюється у формі публічного захисту кваліфікаційної роботи.
Вимоги до єдиного державного кваліфікаційного іспиту	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом вищої освіти зі спеціальності F5 «Кібербезпека та захист інформації».
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має передбачити розв'язання спеціалізованого завдання теоретичного або практичного спрямування в галузі кібербезпеки та захисту інформації з поглибленим вивченням мобільних та відеоінформаційних систем.ації. Кваліфікаційна робота має бути попередньо перевірена на плагіат відповідно до «Положення про запобігання академічному плагіату у Державному університеті інформаційно-комунікаційних технологій». Кваліфікаційна робота має бути оприлюднена (за виключенням робіт, що містять інформацію з обмеженим доступом) на у репозиторії Державного університету інформаційно-комунікаційних технологій.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

К7

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	ОК36	ОК37	ОК38
1		2	4	5	6	7	8	9	10	11	12	13	14	26	32	34	15	16	17	18	19	20	21	22	23	24	25	27	28	29	30	31	33	35	36	37	38	39
ЗК1		+	+	+	+				+				+			+				+	+			+		+			+	+	+	+	+	+	+	+	+	+
ЗК2							+	+		+	+	+		+	+	+	+	+	+			+	+		+		+	+	+	+		+	+	+			+	+
ЗК3	+		+			+		+					+		+																+							
ЗК4														+	+	+					+			+		+			+		+	+			+	+	+	+
ЗК5								+				+	+			+	+	+			+				+	+	+	+		+	+	+	+	+			+	+
ЗК6	+	+		+					+																													
ЗК7			+		+				+		+	+					+						+										+				
СК1								+					+													+								+				+
СК2										+		+			+	+	+	+	+	+		+			+		+	+	+	+	+							
СК3					+											+										+				+	+	+						
СК4					+										+																+							
СК5					+									+	+	+								+					+	+								
СК6														+		+				+				+					+	+	+		+	+				
СК7																+										+			+	+	+	+	+					
СК8															+	+					+								+	+	+		+	+				
СК9															+					+				+					+		+							
СК10																+					+		+						+	+	+	+	+	+				
СК11														+	+						+				+		+		+	+	+			+				
СК12														+	+						+								+	+	+			+				

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

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	ОК36	ОК37	ОК38
1		2	3	4	5	6	7	8	9	10	11	12	13	25	31	33	14	15	16	17	18	19	22	21	22	23	24	26	27	28	29	30	32	34	35	36	37	38
РН 1	+			+					+														+													+		
РН 2		+	+			+																											+					+
РН 3	+																		+						+	+										+	+
РН 4					+																														+			+
РН 5														+																						+		
РН 6		+																									+											+
РН 7												+				+	+												+	+								+
РН 8							+				+			+			+											+										
РН 9								+					+						+					+		+					+			+				
РН 10										+								+		+																		
РН 11					+								+	+										+														
РН 12										+										+			+	+	+													
РН 13																+			+							+						+				+		
РН 14																					+															+		
РН 15															+							+												+		+		
РН 16				+																																		
РН 17													+		+									+												+		
РН 18																+		+									+											
РН 19																																						
РН 20											+																	+	+	+	+	+	+				
РН 21															+						+	+																

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