

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-
КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**«ТЕХНІЧНІ СИСТЕМИ ІНФОРМАЦІЙНОГО ТА
КІБЕРНЕТИЧНОГО ЗАХИСТУ»
ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
першого (бакалаврського) рівня вищої освіти
(оновлена)**

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

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

Протокол № 3 від 17 березня 2026 р.

Наказ № 105 від 20 березня 2026 р.



Ректор

Володимир ШУЛЬГА

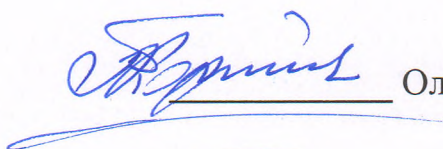
Освітня програма вводиться в дію з 01 вересня 2026 р.

Київ 2026

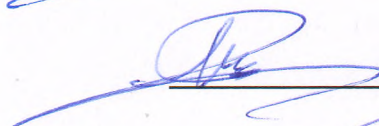
**ЛИСТ ПОГОДЖЕННЯ
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«ТЕХНІЧНІ СИСТЕМИ ІНФОРМАЦІЙНОГО
ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ»**

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

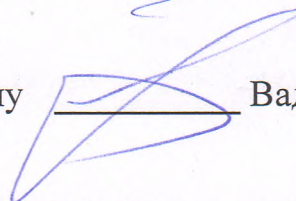
1. Перший проректор

 Олександр КОРЧЕНКО

2. Проректор з навчальної роботи

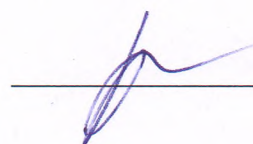
 Артур ГУДМАНЯН

3. Начальник навчально-методичного відділу

 Вадим ВЛАСЕНКО

4. Вчена рада Навчально-наукового інституту кібербезпеки та захисту інформації
Протокол № 8 від «26» лютого 2026 р.

Голова вченої ради ННІКБЗІ

 Євгенія ІВАНЧЕНКО

Кафедра Технічних систем кіберзахисту

Протокол № 9 від «12» лютого 2026 р.

Завідувач кафедри

Технічних систем кіберзахисту

 Олександр ТУРОВСЬКИЙ

Голова студентської ради ННІ КБЗІ

 Станіслав ШТЕФАН

Рецензії від зовнішніх стейкхолдерів:

1. ТОВ «ЛУЧ»;
2. ТОВ «А.Г.Г.»



ПЕРЕДМОВА

Розроблено робочою групою у складі:

Гарант освітньої програми Котенко Андрій Миколайович	кандидат технічних наук, доцент, доцент кафедри Технічних систем кіберзахисту
Члени робочої групи: Туровський Олександр Леонідович	доктор технічних наук, професор, завідуючий кафедрою Технічних систем кіберзахисту
Пепа Юрій Володимирович	кандидат технічних наук, доцент, професор кафедри Технічних систем кіберзахисту
Шуклін Герман Вікторович (представники роботодавців)	кандидат технічних наук, доцент, заступник директора ТОВ «ЛУЧ»
Заболотний Назар Борисович (здобувач вищої освіти)	Студент 4 курсу спеціальності 125 – кібербезпека та захист інформації

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 № 9 від «12» лютого 2026 р.

Введено в дію наказом ректора № 105 від 20 березня 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 та захисту інформації .
Офіційна назва освітньої програми	Освітньо-професійна програма «Технічні системи інформаційного та кібернетичного захисту»
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 № 1118045 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	Оновлена 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 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)	Об'єкти професійної діяльності випускників: - об'єкти інформатизації, а саме: комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-комунікаційні системи та мережі, інформаційні ресурси та технології; - системи та технології забезпечення безпеки інформації; - процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. Теоретичний зміст предметної діяльності. Знання: - законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; - принципів супроводу систем та комплексів кібербезпеки; - теорії, моделей та принципів управління доступом до інформаційних ресурсів; - методів та засобів виявлення та ідентифікації каналів витоку інформації; - методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; - методів та засобів технічного та криптографічного захисту інформації. F «Інформаційні технології». F5 «Кібербезпека та захист інформації».
Орієнтація освітньої програми	Освітня. 100% обсягу освітньої програми спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю F5 «Кібербезпека та захист інформації» визначеного стандартом вищої освіти. Програма носить прикладний характер, спрямована на забезпечення потреб ринку праці.
Основний фокус освітньої	Спеціальна освіта та професійна підготовка в галузі

програми та спеціалізації	інформаційних технологій. Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та кібербезпеки на підприємствах в установах та організаціях. Ключові слова: ІНФОРМАЦІЯ, ЗАГРОЗИ, ВРАЗЛИВОСТІ, ЗАХИЩЕНІСТЬ, КІБЕРБЕЗПЕКА, ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ.
Опис предметної області	Об'єкти професійної діяльності випускників: об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-комунікаційні системи, інформаційні ресурси і технології; технології забезпечення безпеки інформації; процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. Цілі навчання підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. Теоретичний зміст предметної діяльності Знання: законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; теорії, моделей та принципів управління доступом до інформаційних ресурсів; теорії систем управління інформаційною та/або кібербезпекою; методів та засобів виявлення, управління та ідентифікації ризиків; методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; методів та засобів технічного та криптографічного захисту інформації; сучасних інформаційно-комунікаційних технологій; сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; автоматизованих систем проектування. Методи, методики та технології: Методи, методики інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/або кібербезпеки Інструменти та обладнання: системи розробки, забезпечення, моніторингу та контролю інформаційної та/або кібербезпеки; сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

Особливості програми	Програма передбачає: - викладання окремих дисциплін циклу професійної підготовки англійською мовою; - передбачено в межах навчального процесу отримання сертифікатів від провідних компаній в галузі інформаційних технологій; - залучення до проведення практичних занять та лабораторних робіт, фахівців-практиків з кібербезпеки та захисту інформації; - забезпечення умов підготовки здобувачів вищої освіти у реальному середовищі до майбутньої професійної діяльності для набуття відповідних компетенцій, шляхом організації проведення практик (ознайомча, виробнича та переддипломна) в організаціях-партнерів, з можливістю подальшого працевлаштування.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Бакалавр з кібербезпеки та захисту інформації за освітньою програмою «Технічні системи інформаційного та кібернетичного захисту» (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) Існує можливість отримати міжнародні сертифікати в галузі кібербезпеки.
Подальше навчання	Можливість продовжити навчання за освітньою програмою другого (магістерського) освітнього рівня вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Проблемно-орієнтоване навчання. Викладання проводиться державною та іноземною (викладання окремих дисциплін проводиться англійською) мовами, які формують професійні компетенції. Викладання спрямовано на засвоєння знань, умінь і навичок для подальшого застосування у практиці. Основними способами передачі змісту освітньої

	програми є проведення лекцій, семінарських, практичних, індивідуальних, лабораторних занять, консультації, розв'язання ситуаційних задач, тестування, презентації, ознайомча, виробнича, переддипломна практики.
Оцінювання	Оцінювання сформованих компетенцій під час контрольних заходів, які передбачені цією освітньою програмою зазначені у навчальному плані. Критерії оцінювання знань, умінь та навичок розроблені у відповідності до чинного законодавства та висвітлено у Положенні про організацію освітнього процесу у Державному університеті інформаційно-комунікаційних технологій.
6 – Програмні компетенції	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області та розуміння професії. ЗК3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК5. Здатність до пошуку, оброблення та аналізу інформації. ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в 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 зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства

	на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Спеціальності (фахові предметні компетентності) (СК)	СК1. Здатність застосовувати законодавчу та нормативно- правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. СК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. СК5. Здатність відновлювати функціонування Інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. СК6. Здатність впроваджувати та забезпечувати функціонування інформації комплексних (комплекси систем нормативно-правових, захисту організаційних та технічних засобів і методів, процедур, практичних прийомів тощо). СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

7 – Програмні результати навчання

Результати навчання (РН)

- РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.
- РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.
- РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.
- РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
- РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
- РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
- РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
- РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
- РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
- РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
- РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з

урахування вимог до захисту інформації.

RH12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

RH13. 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.

RH14. Вирішувати задачі управління процесами відновлення штатног о 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.

RH15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

RH16. Вирішувати задачі впровадження та супроводу комплексних інформаційних системах.

RH17. 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.

RH18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

RH19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

RH20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту

	інформації. РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації інформаційних системах.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Всі науково-педагогічні працівники, залучені до реалізації освітньої складової освітньо-професійної програми є штатними співробітниками Державного університету інформаційно-комунікаційних технологій, мають підтверджений рівень наукової і професійної активності. Група забезпечення освітньо-професійної програми сформована з числа науково-педагогічних працівників Державного університету інформаційно-комунікаційних технологій. Кількісний та якісний склад групи відповідають Ліцензійним вимогам
Матеріально-технічне забезпечення	Для проведення практичних та лабораторних занять з метою формування спеціальних компетентностей зі спеціальності F5 Кібербезпека та захист інформації спеціалізації Технічні системи інформаційного та кібернетичного захисту використовуються спеціалізовані лабораторії університету, які оснащені сучасними комп'ютерами, програмно-апаратними комплексами та спеціалізованим обладнанням. НАВЧАЛЬНА ЛАБОРАТОРІЯ ЗАСОБІВ КОНТРОЛЮ ДОСТУПУ – забезпечує проведення практичних занять з питань контролю та управління доступом, використання автономних біометричних терміналів, мережних контролерів, програмно-апаратних комплексів систем відеоспостереження HikVision та Ajax. НАВЧАЛЬНА ЛАБОРАТОРІЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ «РІАС» – забезпечує проведення практичних занять з питань технічного захисту конфіденційної інформації на об'єктах інформаційної діяльності від витоку акустичним, віброакустичним та електромагнітним каналами з використанням широкосмугових генераторів акустичного та електромагнітного шуму,

	забезпечення вивчення порядку застосування пошукового програмно-апаратного комплексу DigiScan EX; методів виявлення випромінювань за допомогою індикаторів поля типу PROTEKT; порядку застосування скануючих приймачів AR 8200, IC-R5, IC-R2500 та локатора нелінійностей NR-900 EM.
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, електронної бібліотеки університету та системи дистанційного навчання Google Classroom.
9 – Академічна мобільність	
Національна кредитна мобільність	Наявність двосторонніх договорів між Державним університетом інформаційно-комунікаційних технологій та закладами вищої освіти України забезпечує національну кредитну мобільність.
Міжнародна кредитна мобільність	Зміст навчання відповідає світовим освітнім стандартам, що дозволяє приймати участь у програмах подвійних дипломів та бути конкурентоспроможним на світовому ринку праці.
Навчання іноземних здобувачів вищої освіти	Дозволяє можливість навчання іноземним громадянам.

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

2.1. Зміст підготовки за освітньою програмою компетентності та результатами навчання

№ п.п.	Дисципліна	Код н/д	Компетентність	Результат навчання
1. Цикл дисциплін загальної підготовки				
1.	Теоретична підготовка базової загальновійськової підготовки	OK1	ЗК1, ЗК6, ЗК8	РН3, РН6,
2.	Вища математика	OK2	ЗК5	РН7, РН8
3.	Основи управління інформаційною та кібербезпекою	OK3	СК1, СК7	РН4, РН9, РН11, РН14, РН17
4.	Бізнес процеси в кібербезпеці	OK4	ЗК1, ЗК2, ЗК7, СК3	РН1, РН3, РН4, РН6
5.	Філософія	OK5	ЗК3,	РН1, РН9
6.	Англійська мова для професійної комунікації	OK6	ЗК4, СК1	РН1
7.	Українська мова за професійним спрямуванням	OK7	ЗК2, ЗК3	РН1, РН9
8.	Комунікації в кібербезпеці	OK8	ЗК1, ЗК2, ЗК6, ЗК7	РН1, РН3, РН4, РН5
9.	Соціально-екологічна безпека життєдіяльності	OK9	ЗК2 ЗК6, ЗК7, ЗК8, СК2	РН3, РН6
10.	Фізика	OK10	ЗК2, ЗК5, ЗК7	РН1, РН7, РН8
11.	Нормативно-правове забезпечення інформаційної безпеки	OK11	ЗК2, ЗК6, СК1, СК3	РН2, РН9 РН19
12.	Теорія інформації та кодування	OK12	ЗК1, ЗК5, СК2, СК6,	РН7, РН8
1. Цикл дисциплін професійної та практичної підготовки				
1.	Теорія кіл і сигналів в інформаційному та кіберпросторах	OK13	ЗК2, ЗК5, СК2	РН5, РН9, РН20
2.	Прикладне програмування	OK14	ЗК2, ЗК5, СК2,	РН6, РН8, РН20
3.	Основи кібербезпеки та захисту інформації	OK15	ЗК2, СК2	РН5, РН6
4.	Безпека інформаційно-комунікаційних систем	OK16	ЗК1, ЗК2, СК2, СК5, СК6,	РН5, РН10, РН12, РН16
5.	Стандарти інформаційної та кібербезпеки	OK17	ЗК4, ЗК5, СК8, СК10	РН3, РН11

6.	Прикладна криптологія	OK18	ЗК2, СК2, СК8	PH5, PH7, PH19
7.	Аналіз та оцінка уразливостей інформаційних систем	OK19	ЗК2, СК1, СК4, СК10	PH5, PH10, PH4, PH16
8.	Англійська мова: комунікативний практикум	OK20	ЗК4, СК1	PH1, PH9
9.	Комплексні системи захисту інформації	OK21	ЗК2, ЗК5, СК2, СК10	PH4, PH5, PH11, PH14, PH16, PH17, PH20, PH21
10.	Компонентна база в системах захисту інформації	OK22	ЗК2, ЗК5, СК2, СК5, СК6	PH5, PH8, PH20,
11.	Поля і хвилі в системах технічного захисту інформації	OK23	ЗК2, СК5, СК6, СК9	PH12, PH14, PH15, PH20
12.	Засоби передачі в системах технічного захисту інформації	OK24	ЗК2, ЗК5, СК2, СК5, СК6, СК10	PH4, PH5, PH6, PH14, PH19
13.	Засоби прийому та обробки сигналів в системах технічного захисту інформації	OK25	ЗК1, ЗК2, ЗК5, СК2, СК5, СК6, СК10	PH4, PH5, PH6, PH14, PH19, PH20
14.	Методи та засоби технічного захисту інформації	OK26	ЗК1, ЗК2, ЗК5, СК6, СК10	PH4, PH5, PH10, PH12, PH16, PH20, PH21
15.	Схемотехніка пристроїв технічного захисту інформації	OK27	ЗК1, ЗК2, ЗК4, СК6, СК10	PH4, PH5, PH6, PH8, PH20
16.	SIEM системи	OK28	ЗК1, ЗК2, ЗК4, ЗК5, СК5, СК6, СК10	PH2, PH5, PH10, PH13
17.	Метрологія та вимірювання в інформаційній безпеці	OK29	ЗК2, ЗК3, ЗК4, СК1, СК2, СК10	PH4, PH8, PH20
18.	Технічні засоби охорони об'єктів	OK30	ЗК1, ЗК2, ЗК5, СК6, СК7, СК10	PH4, PH6, PH8, PH10, PH13, PH19
19.	Аудит системи менеджменту інформаційної безпеки	OK31	ЗК1, ЗК2, ЗК4, ЗК5, СК2, СК6, СК7, СК8, СК10	PH3, PH4, PH9, PH10, PH12, PH17, PH19, PH20
20.	Програмування в кібербезпеці	OK32	ЗК1, ЗК2, ЗК5, ЗК7, СК2, СК6, СК8	PH4, PH7, PH13, PH18, PH19
21.	Ознайомча практика	OK33	ЗК1, ЗК2, ЗК4, СК1, СК2,	PH3, PH4, PH6, PH9
22.	Виробнича практика	OK34	ЗК1, ЗК2, ЗК4, ЗК8, СК1, СК2,	PH3, PH4, PH6, PH9, PH10, PH12, PH19, PH20
23.	Переддипломна практика	OK35	ЗК1, ЗК2, ЗК4, ЗК5, ЗК8, СК1, СК2, СК3, СК5, СК7, СК8, СК10	PH3, PH4, PH7, PH9, PH11, PH12, PH19, PH20
24.	Кваліфікаційна робота	OK36	ЗК1, ЗК2, ЗК4, ЗК5, СК1, СК4, СК5, СК6, СК7, СК10	PH2, PH3, PH4, PH6, PH7, PH9, PH10, PH11, PH12, PH14,

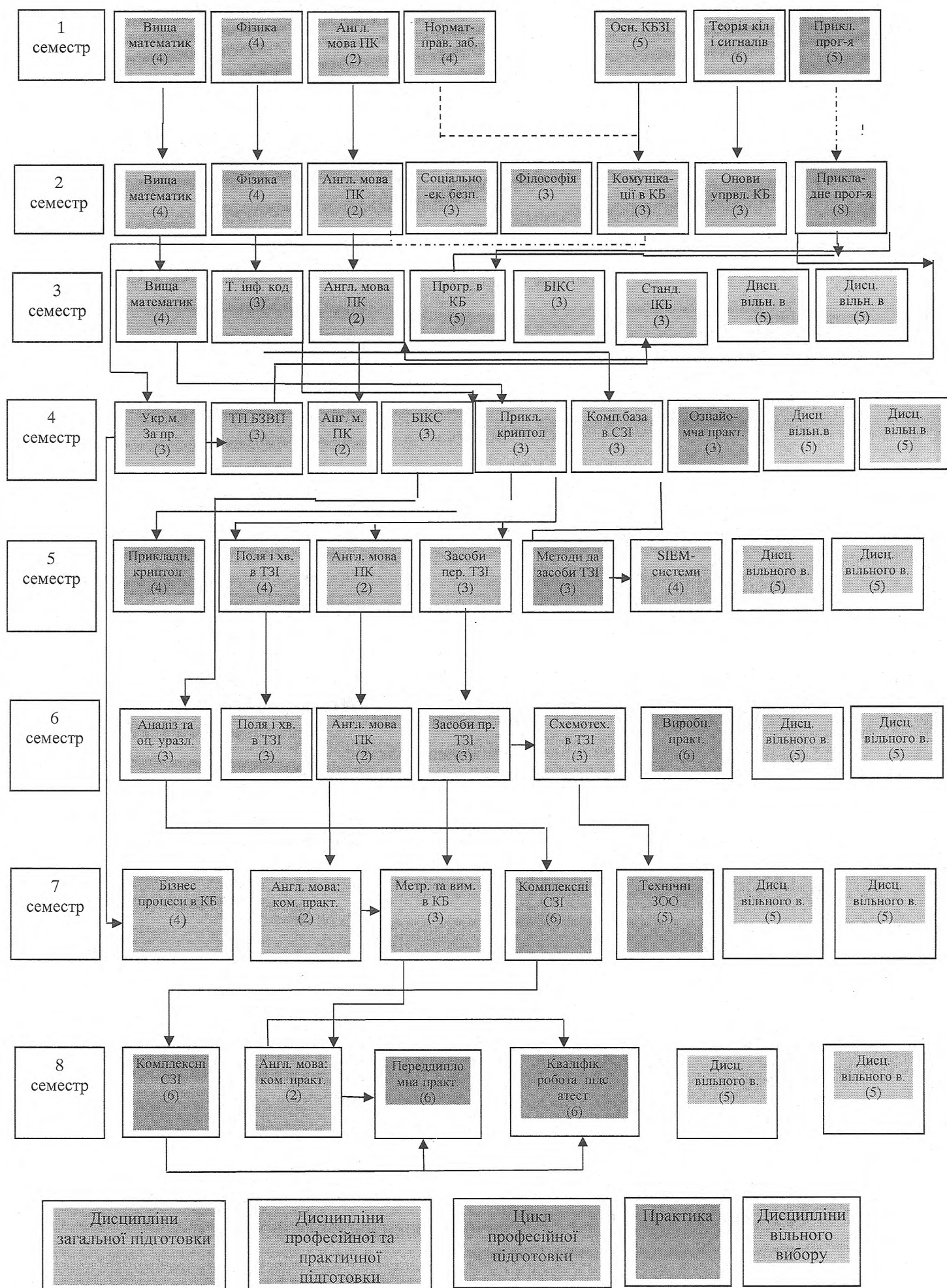
				PH15, PH16, PH9
2. Дисципліни вільного вибору студента				
1.	Дисципліна вільного вибору студента	BK1		
2.	Дисципліна вільного вибору студента	BK2		
3.	Дисципліна вільного вибору студента	BK3		
4.	Дисципліна вільного вибору студента	BK4		
5.	Дисципліна вільного вибору студента	BK5		
6.	Дисципліна вільного вибору студента	BK6		
7.	Дисципліна вільного вибору студента	BK7		
8.	Дисципліна вільного вибору студента	BK8		
9.	Дисципліна вільного вибору студента	BK9		
10.	Дисципліна вільного вибору студента	BK10		
11.	Дисципліна вільного вибору студента	BK11		
12.	Дисципліна вільного вибору студента	BK12		

*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			
OK1	Теоретична підготовка базової загальновійськової підготовки	3	Залік
OK2	Вища математика	12	Залік, Іспит
OK3	Основи управління кібернетичною безпекою	3	Залік
OK4	Бізнес процеси в кібербезпеці	4	Залік
OK5	Філософія	3	Залік
OK6	Англійська мова для професійної комунікації	12	Залік, Іспит
OK7	Українська мова за професійним спрямуванням	3	Залік
OK8	Комунікації в кібербезпеці	6	Залік
OK9	Соціально-екологічна безпека життєдіяльності	3	Іспит
OK10	Фізика	8	Залік, Іспит
OK11	Нормативно-правове забезпечення інформаційної безпеки	4	Іспит
OK12	Теорія інформації та кодування	3	Іспит
OK13	Теорія кіл і сигналів в інформаційному та кіберпросторах	6	Іспит
OK14	Прикладне програмування	13	Залік, Іспит
OK15	Основи кібербезпеки та захисту інформації	3	Залік
OK16	Безпека інформаційно-комунікаційних систем	7	Залік, Іспит
OK17	Стандарти інформаційної та кібербезпеки	4	Іспит
OK18	Прикладна криптологія	6	Залік, Іспит
OK19	Аналіз та оцінка уразливостей інформаційних систем	3	Іспит
OK20	Англійська мова: комунікативний практикум	4	Залік
OK21	Комплексні системи захисту інформації	12	Залік, Іспит
OK22	Компонентна база в системах захисту інформації	3	Іспит
OK23	Поля і хвилі в системах технічного захисту інформації	6	Залік, Іспит, КІП
OK24	Засоби передачі в системах технічного захисту інформації	3	Залік
OK25	Засоби прийому та обробки сигналів в системах технічного захисту інформації	3	Залік
OK26	Методи та засоби технічного захисту інформації	3	Залік
OK27	Схемотехніка пристроїв технічного захисту інформації	3	Іспит
OK28	SIEM системи	3	Залік
OK29	Метрологія та вимірювання в інформаційній безпеці	3	Іспит
OK30	Технічні засоби охорони об'єктів	3	Іспит
OK31	Аудит системи менеджменту інформаційної безпеки	3	Залік
OK32	Програмування в кібербезпеці	3	Залік
OK33	Ознайомча практика	3	Залік

OK34	Виробнича практика	6	Залік
OK35	Переддипломна практика	6	Залік
OK36	Кваліфікаційна робота	6	
Загальний обсяг обов'язкових компонент:		180	
Вибіркові компоненти ОП			
Дисципліна вільного вибору студента		5	Залік
Дисципліна вільного вибору студента		5	Залік
Дисципліна вільного вибору студента		5	Залік
Дисципліна вільного вибору студента		5	Залік
Дисципліна вільного вибору студента		5	Залік
Дисципліна вільного вибору студента		5	Залік
Дисципліна вільного вибору студента		5	Залік
Дисципліна вільного вибору студента		5	Залік
Дисципліна вільного вибору студента		5	Залік
Дисципліна вільного вибору студента		5	Залік
Дисципліна вільного вибору студента		5	Залік
Дисципліна вільного вибору студента		5	Залік
Загальний обсяг вибіркових компонент:		60	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		240	



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 спеціалізованої задачі в галузі інформаційної та кібербезпеки. Кваліфікаційна робота має бути попередньо перевірена на плагіат відповідно до «Положення про систему запобігання та виявлення академічного 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

	OK1	OK2	OK3	OK4	OK5	OK6	OK7	OK8	OK9	OK10	OK11	OK12	OK13	OK14	OK15	OK16	OK17	OK18	OK19	OK20	OK21	OK22	OK23	OK24	OK25	OK26	OK27	OK28	OK29	OK30	OK31	OK32	OK33	OK34	OK35	OK36		
3K1	+			+				+				+				+										+	+	+	+		+	+	+	+	+	+	+	
3K2				+	+		+	+	+	+	+		+	+	+	+		+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		
3K3						+	+									+				+										+								
3K4																	+		+						+		+	+	+		+		+	+	+	+		
3K5		+					+			+		+	+	+			+				+	+		+		+	+	+		+	+	+			+	+		
3K6	+							+	+		+																											
3K7		+		+				+	+	+																							+					
3K8	+								+																										+	+		
CK1			+			+					+								+	+		+							+			+	+	+	+	+		
CK2									+			+	+	+	+	+		+			+			+	+				+		+	+	+	+	+			
CK3				+							+																		+			+			+	+		
CK4																			+																		+	
CK5																+						+	+	+	+	+	+		+							+	+	
CK6												+				+						+	+	+	+	+	+		+		+	+	+				+	
CK7			+																										+		+	+					+	+
CK8																	+	+														+	+			+		
CK9																							+			+	+				+							
CK10																	+		+		+			+	+	+	+	+	+	+	+					+	+	

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

	OK1	OK2	OK3	OK4	OK5	OK6	OK7	OK8	OK9	OK10	OK11	OK12	OK13	OK14	OK15	OK16	OK17	OK18	OK19	OK20	OK21	OK22	OK23	OK24	OK25	OK26	OK27	OK28	OK29	OK30	OK31	OK32	OK33	OK34	OK35	OK36
PH 1				+	+		+	+		+																										
PH 2						+					+									+								+								+
PH 3	+			+				+	+								+														+		+	+	+	+
PH 4			+	+				+													+				+	+	+	+		+	+	+	+	+	+	+
PH 5								+					+	+	+	+		+	+		+	+		+	+	+	+	+	+							
PH 6	+			+					+						+									+	+		+						+	+		+
PH 7		+								+		+						+														+			+	+
PH 8		+								+		+	+	+								+						+		+						
PH 9			+		+		+				+						+			+												+		+	+	+
PH 10																+			+							+	+			+				+		+
PH 11			+														+				+														+	+
PH 12																+							+			+					+			+	+	+
PH 13																			+					+			+					+				
PH 14			+																		+		+	+	+			+							+	
PH 15																			+				+													+
PH 16																+					+					+								+		+
PH 17			+																		+										+					
PH 18																		+														+				
PH 19											+								+					+	+						+	+				
PH 20													+								+	+				+								+	+	+
PH 21														+					+		+		+		+	+	+	+	+	+			+	+		

Гарант освітньої програми

Доцент кафедри Технічних систем кіберзахисту,
Навчально-наукового
інституту кібербезпеки та захисту інформації
Державного університету
інформаційно-комунікаційних технологій,
кандидат технічних наук, доцент



Андрій КОТЕНКО