



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-
КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ОСВІТНЯ ПРОГРАМА
«ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА БЕЗПЕКА»
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 УНІВЕРСИТЕТУ
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.



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

спеціальність	F5 Кібербезпека та захист інформації
галузь знань	F Інформаційні технології
рівень вищої освіти	перший (бакалавр)
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 2026р.

Голова Вченої Ради ННІКБЗІ  Євгенія ІВАНЧЕНКО

5. Кафедра систем та технологій кібербезпеки

Протокол № 4/1 від «25» лютого 2026р.

Завідувач кафедри систем та технологій кібербезпеки

 Галина ГАЙДУР

6. Голова студентської ради ННІКБЗІ  Станіслав ШТЕФАН

Рецензії від зовнішніх стейкхолдерів:

1. ТОВ «Центр інформаційної та технічної підтримки «Сапфоріс»» (ESET in Ukraine).
2. КНУБА

ПЕРЕДМОВА

Розроблено робочою групою у складі:

Гарант освітньої програми (голова робочої групи)

Сергій ГАХОВ – кандидат військових наук, доцент, доцент кафедри систем та технологій кібербезпеки.

Члени робочої групи:

Галина ГАЙДУР – доктор технічних наук, професор, завідувач кафедри систем та технологій кібербезпеки;

Віталій МАРЧЕНКО – доктор філософії, доцент кафедри систем та технологій кібербезпеки;

Єгор ЛАЗАРЄВ – здобувач 4-го курсу освітньої програми «Інформаційна та кібернетична безпека»;

Олександр ІЛЮША - ТОВ «Центр інформаційної та технічної підтримки «Сапфоріс»» (ESET in Ukraine).

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 систем та технологій кібербезпеки

протокол № від « » 2026 р.

Введено в дію наказом ректора № ___ від _____ 20__ року.

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 – <i>бакалавр з кібербезпеки та захисту інформації</i>
Офіційна назва освітньої програми	Освітня програма «Інформаційна та кібернетична безпека».
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний: – на базі повної загальної середньої освіти. Обсяг освітньої програми - 240 кредитів ЄКТС; термін навчання 3 роки та 10 місяців денної форми навчання та 4 роки 10 місяців заочної форми навчання. – на базі ступеня молодшого бакалавра, фахового молодшого бакалавра або освітньо-кваліфікаційного рівня молодшого спеціаліста здійснюється в порядку, визначеному законодавством, при перезарахуванні не більше ніж 60 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки фахівців.
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	Для здобуття освітнього ступеня бакалавра зі спеціальності F5 Кібербезпека та захист інформації можуть вступати особи, які здобули повну загальну середню освіту. Прийом на основі здобутого ступеня молодшого бакалавра, фахового молодшого бакалавра або освітньо-кваліфікаційного рівня молодшого спеціаліста здійснюється в порядку, визначеному законодавством.
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	https://duikt.edu.ua/ua/1822-osvitno-profesiyni-programi-kafedra-informaciynoi-ta-kibernetichnoi-bezpeki

2 – Мета освітньої програми

Метою бакалаврської програми є підготовка фахівців здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації, які матимуть здатність розв'язувати складні задачі у галузі кібербезпеки та захисту інформації, з правом подальшої професійної діяльності у державних та комерційних підприємствах та організаціях за спеціальністю.

3 – Характеристика освітньої програми

Предметна область, напрям (галузь знань, спеціальність)	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. Підготовка фахівців здатних використовувати і впроваджувати технології інформаційної та кібернетичної безпеки. Ключові слова: КІБЕРБЕЗПЕКА. ІНФОРМАЦІЯ, КІБЕРЗАХИСТ, ІНЦИДЕНТИ, МЕТОДИ ТА ЗАСОБИ
Опис предметної області	Об'єкти професійної діяльності випускників: - технології кібербезпеки та захисту інформації; - процеси управління кібербезпекою та захистом інформації; об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології. Цілі навчання підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації. Теоретичний зміст предметної діяльності Принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і

	<p>потенційних загроз національній безпеці України у кіберпросторі.</p> <p>Методи, методики та технології: методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації.</p> <p>Інструменти та обладнання: засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).</p>
<p>Особливості програми</p>	<p>Програма передбачає:</p> <ul style="list-style-type: none"> - 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.
<p>4 – Придатність випускників до працевлаштування та подальшого навчання</p>	
<p>Придатність до працевлаштування</p>	<p>Бакалавр з кібербезпеки та захисту інформації за освітньою програмою «Інформаційна та кібернетична безпека» (випускник) здатний виконувати професійні роботи за Державним класифікатором професій ДК 003: 2010:</p> <p>Основна: 2139.2 Фахівець з підтримки інфраструктури кіберзахисту. Фахівець з реагування на інциденти кібербезпеки. Молодший адміністратор мереж і систем. За умови отримання сертифікату у кваліфікаційному центрі.</p>

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, теоретична підготовка з базової загальної військової підготовки.
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)	<p>ЗК1. Здатність застосовувати знання у практичних ситуаціях</p> <p>ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності</p> <p>ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.</p> <p>ЗК4. Здатність спілкуватися іноземною мовою.</p> <p>ЗК5. Здатність вчитися і оволодівати сучасними знаннями.</p> <p>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 та свобод людини і громадянина в Україні.</p> <p>ЗК7. Здатність ухвалювати рішення й діяти</p>

	<p>дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.</p> <p>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.</p>
<p>Спеціальні (фахові предметні компетентності)</p>	<p>СК1. Здатність застосовувати законодавчу та нормативно- правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.</p> <p>СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.</p> <p>СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.</p> <p>СК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.</p> <p>СК5. Здатність відновлювати функціонування Інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.</p> <p>СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)</p> <p>СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.</p> <p>СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою юрмаційної безпеки.</p>

7 – Програмні результати навчання

- 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.
- 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 й 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 систем захисту інформації в 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.

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

	<p>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 в інформаційних системах.</p>
<p>8 – Ресурсне забезпечення реалізації програми</p>	
<p>Кадрове забезпечення</p>	<p>Група забезпечення спеціальності 125 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.</p>
<p>Матеріально-технічне забезпечення</p>	<p>Теоретичні заняття проводяться в сучасних комп'ютерних класах та спеціалізованих лабораторіях, які оснащені спеціалізованими апаратно-програмними засобами.</p> <p>НАВЧАЛЬНА ЛАБОРАТОРІЯ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ</p> <p>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 в корпоративних інформаційних системах.</p> <p>НАВЧАЛЬНА ЛАБОРАТОРІЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК</p> <p>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.</p> <p>Спеціалізований програмно-апаратний комплекс ESET Protect дозволяє відпрацьовувати навички для захисту кінцевих точок.</p> <p>НАВЧАЛЬНА ЛАБОРАТОРІЯ МЕРЕЖЕВОЇ БЕЗПЕКИ</p> <p>Лабораторія призначена для вивчення технологій мережевої безпеки CISCO та HUAWEI з можливістю</p>

	<p>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.</p>
Інформаційне та навчально-методичне забезпечення	<p>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.</p>
9 – Академічна мобільність	
Національна кредитна мобільність	<p>Наявність двосторонніх договорів між Державним університетом інформаційно-комунікаційних технологій та закладами вищої освіти України забезпечує національну кредитну мобільність.</p>
Міжнародна кредитна мобільність	<p>Зміст навчання відповідає світовим освітнім стандартам, що дозволяє приймати участь у програмах подвійних дипломів та бути конкурентоспроможним на світовому ринку праці.</p>
Навчання іноземних здобувачів вищої освіти	<p>Дозволяє можливість навчання іноземним громадянам.</p>

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

2.1. Зміст підготовки за освітньою програмою компетентності та результатами навчання

№ п.п.	Дисципліна	Шифр	Компетентність	Результат навчання
1. Цикл дисциплін загальної підготовки				
1.	Вища математика	OK01	ІК, ЗК 5	PH8
2.	Фізика	OK02	ІК, ЗК5	PH8
3.	Англійська мова для професійної комунікації*	OK03	ІК, ЗК4	PH2
4.	Англійська мова: комунікативний практикум*	OK04	ІК, ЗК4	PH2
5.	Соціально-екологічна безпека життєдіяльності	OK05	ІК, ЗК2, ЗК6, ЗК7, ЗК8	PH3, PH6
6.	Кінцеві пристрої інформаційних систем	OK06	ІК, ЗК2, ЗК8	PH6
7.	Філософія	OK07	ІК, ЗК3	PH1
8.	Українська мова за професійним спрямуванням	OK8	ІК, ЗК3	PH1
9.	Теоретична підготовка базової загальновійськової підготовки	OK9	ІК, ЗК3, ЗК6, ЗК8	PH1, PH3
10.	Бізнес аналітика в кібербезпеці	OK10	ІК, ЗК1, ЗК2	PH4
2. Цикл дисциплін професійної та практичної підготовки				
1.	Основи кібербезпеки	OK11	ІК, ЗК2, ЗК8	PH6
2.	Нормативно-правове забезпечення інформаційної безпеки	OK12	ІК, СК1, ЗК6	PH9
3.	Комунікації в кібербезпеці та захисті інформації	OK13	ІК, ЗК1, ЗК2, ЗК6, ЗК7	PH3, PH4
4.	Теорія кіл і сигналів в інформаційному та кіберпросторах	OK14	ІК, ЗК1, ЗК2, ЗК5, СК9	PH5, PH8, PH20
5.	Прикладне програмування	OK15	ІК, ЗК1, ЗК2, ЗК 5	PH5, PH8
6.	Стандарти кібербезпеки та захисту інформації	OK16	ІК, ЗК 6, СК1	PH9

7.	Теорія інформації та кодування	OK17	ІК, ЗК1, ЗК 8	PH7
8.	Захист від шкідливого програмного засобу	OK18	ІК, СК2, СК4	PH10, PH12, PH13
9.	Аналіз та оцінка уразливостей інформаційних систем	OK19	ІК, СК 10	PH21
10.	Прикладна криптологія	OK20	ІК, ЗК1, ЗК8, СК8	PH7, PH18, PH19
11.	Теоретичні основи захищених інформаційно-комунікаційних технологій	OK21	ІК, СК2, СК5	PH10, PH14, PH15
12.	SIEM системи	OK22	ІК, СК2, СК4	PH10, PH12, PH13
13.	Політики безпеки	OK23	ІК, СК3	PH11
14.	Теорія ризиків	OK24	ІК, СК7	PH17
15.	Захист від несанкціонованого доступу	OK25	ІК, СК2, СК4	PH10, PH12, PH13
16.	Система менеджменту інформаційної безпеки	OK26	ІК, СК3, СК7	PH11, PH17
17.	Основи захисту конфіденційних даних	OK27	ІК, СК4	PH12, PH13
18.	Основи безпеки комп'ютерних мереж	OK28	ІК, СК2, СК4	PH10, PH12, PH13
19.	Безпека Web-ресурсів	OK29	ІК, СК2, СК4	PH10, PH12, PH13
20.	Профілі безпеки	OK30	ІК, СК6, СК9	PH16, PH20
21.	Штучний інтелект в кібербезпеці	OK31	ІК, ЗК1, ЗК2, СК2	PH5, PH10
22.	Інфраструктура відкритих ключів	OK32	ІК, СК2, СК4	PH10, PH12, PH13
23.	Основи реагування на інциденти	OK33	ІК, СК2, СК4, СК5	PH10, PH12, PH15
24.	Аудит систем менеджменту інформаційної безпеки	OK34	ІК, СК 10	PH21
25.	Цифрова криміналістика	OK35	ІК, СК2, СК5	PH10, PH14, PH15
26.	Ознайомча практика	OK36	ІК, ЗК1, ЗК2, ЗК6, ЗК8, СК1, СК2	PH4, PH6, PH9, PH10
27.	Виробнича практика	OK37	ІК, ЗК1, ЗК2, ЗК6, ЗК7, ЗК8, СК1, СК2, СК4	PH3, PH4, PH6, PH9, PH10, PH12, PH13
28.	Переддипломна практика	OK38	ІК, ЗК1, ЗК2, ЗК6, ЗК7, ЗК8, СК1, СК2, СК4, СК5, СК8, СК10	PH3, PH4, PH6, PH9, PH10, PH12, PH13, PH14, PH15, PH18, PH19, PH21
29.	Кваліфікаційна робота	OK39	ІК, ЗК1, ЗК2, ЗК 6, ЗК7, ЗК 8, СК2, СК4, СК5, СК8, СК10	PH3, PH4, PH6, PH9, PH10, PH12, PH13, PH14, PH15, PH18, PH19, PH21

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			

*Англійська 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			
OK01	Вища математика	12	Залік, Залік, Іспит
OK02	Фізика	8	Залік, Іспит
OK03	Англійська мова для професійної комунікації*	12	Залік, Іспит
OK04	Англійська мова: комунікативний практикум	4	Залік, Іспит
OK05	Соціально-екологічна безпека життєдіяльності	3	Залік
OK06	Кінцеві пристрої інформаційних систем	4	Іспит
OK07	Філософія	3	Залік
OK8	Українська мова за професійним спрямуванням **	3	Залік
OK9	Теоретична підготовка базової загальновійськової підготовки *	3	Залік
OK10	Бізнес аналітика в кібербезпеці	3	Залік
OK11	Основи кібербезпеки	3	Іспит
OK12	Нормативно-правове забезпечення інформаційної безпеки	3	Іспит
OK13	Комунікації в кібербезпеці та захисті інформації	4	Залік
OK14	Теорія кіл і сигналів в інформаційному та кіберпросторах	5	Іспит
OK15	Прикладне програмування	12	Залік, Іспит
OK16	Стандарти кібербезпеки та захисту інформації**	3	Іспит
OK17	Теорія інформації та кодування***	4	Іспит

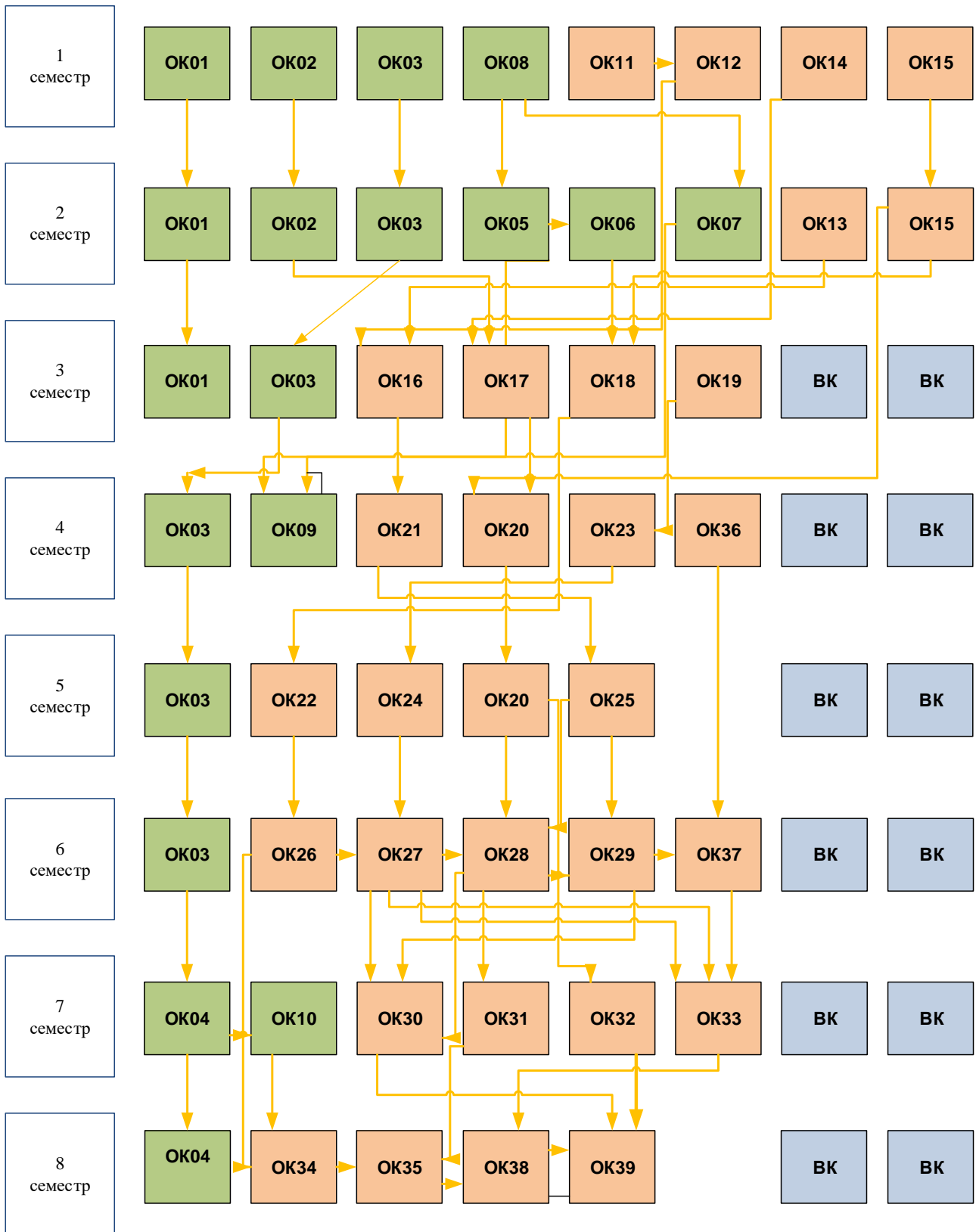
OK18	Захист від шкідливого програмного засобу	4	Іспит
OK19	Аналіз та оцінка уразливостей інформаційних систем	3	Залік
OK20	Прикладна криптологія	10	Залік, Іспит
OK21	Теоретичн і основи захищених інформаційно-комунікаційних технологій	4	Залік
OK22	SIEM системи	5	Іспит
OK23	Політики безпеки	3	Іспит
OK24	Теорія ризиків	3	Залік
OK25	Захист від несанкціонованого доступу	5	Іспит
OK26	Система менеджменту інформаційної безпеки	3	Залік
OK27	Основи захисту конфіденційних даних	3	Іспит
OK28	Основи безпеки компю'терних мереж	3	Іспит
OK29	Безпека Web-ресурсів	3	Іспит
OK30	Профілі безпки	5	Іспит
OK31	Штучний інтелект в кібербезпеці	3	Залік
OK32	Інфраструктура відкритих ключів	4	Іспит
OK33	Основи реагування на інциденти	3	Іспит
OK34	Аудит систем менеджменту інформаційної безпеки	3	Іспит
OK35	Цифрова криміналістика	3	Іспит
OK36	Організаційна практика	3	Залік
OK37	Виробнича практика	6	Залік
OK38	Переддипломна практика	6	Залік
OK39	Кваліфікаційна робота	6	
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 вибірових компонент:		60	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		240	

* Для денної форми навчання

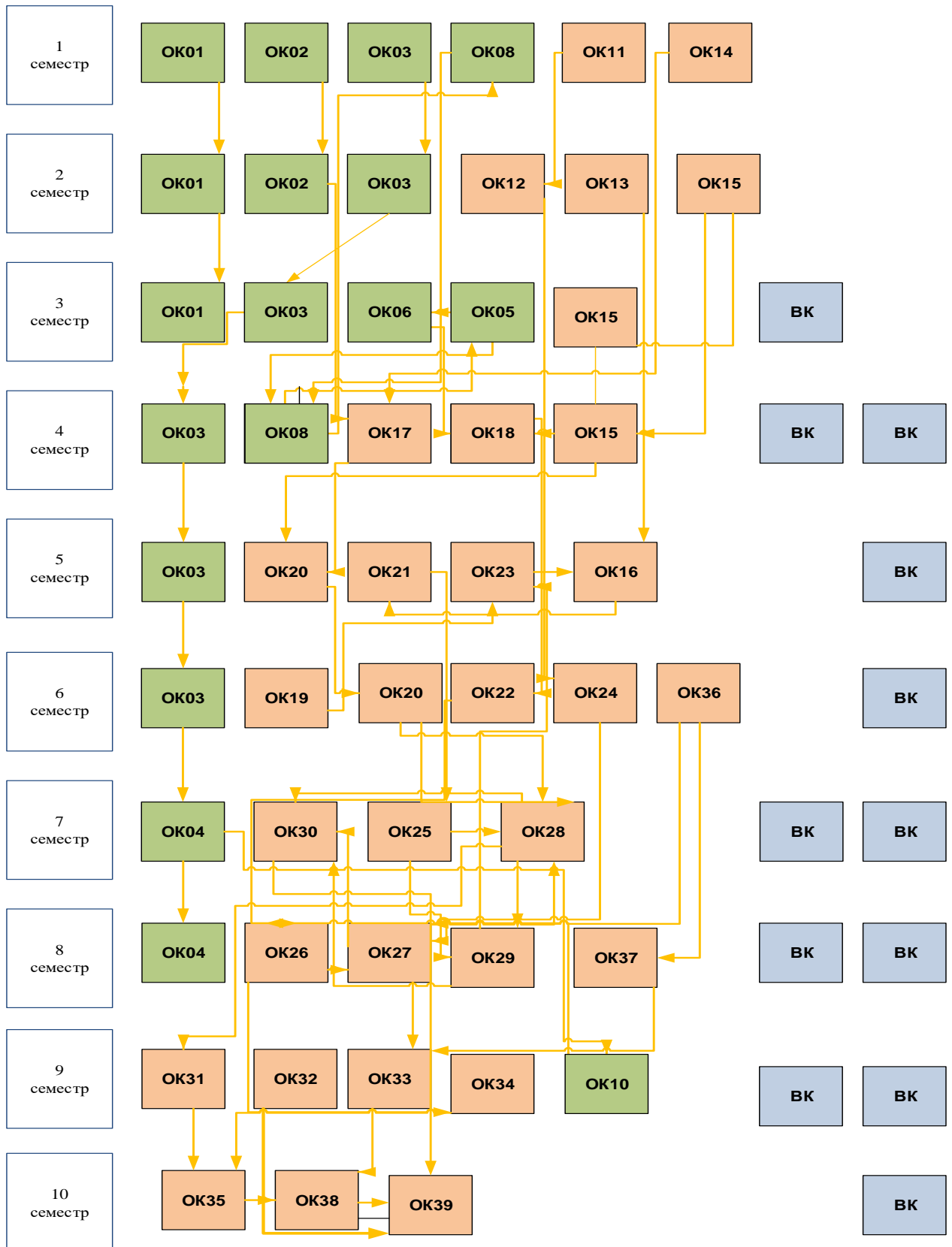
**Для заочної форми навчання обсяг кредитів – 4 ECTS

*** Для заочної форми навчання обсяг кредитів – 5 ECTS

2.3. Структурно-логічна схема ОП



Заочна



3. Форма атестації здобувачів вищої освіти

<i>Форми атестації здобувачів вищої освіти</i>	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту та публічного захисту кваліфікаційної роботи.
<i>Вимоги до єдиного державного кваліфікаційного іспиту</i>	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених цим стандартом.
<i>Вимоги до кваліфікаційної роботи</i>	Кваліфікаційна робота має передбачити розв'язання спеціалізованої задачі в галузі кібербезпеки та захисту інформації. Має бути перевірено на плагіат відповідно «Положення про запобігання академічному плагіату у Державному університеті інформаційно-комунікаційних технологій». Кваліфікаційна робота має бути оприлюднена у репозитарії Державного університету інформаційно-комунікаційних технологій.

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

	OK01	OK02	OK03	OK04	OK05	OK06	OK07	OK08	OK09	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	OK37	OK38	OK39			
PH1								•	•																																	
PH2			•	•																																						
PH3					•				•				•																									•	•	•		
PH4										•			•																										•	•	•	
PH5															•	•																								•		
PH6					•	•	•					•																											•	•	•	•
PH7																		•			•																					
PH8	•	•													•	•																										
PH9												•				•																								•	•	•
PH10																		•			•	•				•			•	•		•	•	•			•	•	•	•		
PH11																						•					•															
PH12																		•				•				•		•	•	•									•	•	•	
PH13																		•				•				•		•	•	•										•	•	•
PH14																					•																			•	•	
PH15																					•																			•	•	
PH16																																										
PH17																																										
PH18																					•																			•	•	
PH19																					•																			•	•	
PH20															•																									•	•	
PH21																																								•	•	

Гарант освітньої програми

Доцент кафедри Систем та технологій кібербезпеки

Навчально-наукового інституту кібербезпеки та захисту інформації

Державного університету інформаційно-комунікаційних технологій

К.військ.наук, доцент

Сергій ГАХОВ

РЕЦЕНЗІЯ

на освітня програму
«Інформаційна та кібернетична безпека»
першого (бакалаврського) рівня вищої освіти
за спеціальністю F5 «Кібербезпека та захист інформації»
Державного університету інформаційно-комунікаційних технологій

Освітньо-професійна програма «Інформаційна та кібернетична безпека» відповідає сучасним вимогам ринку праці у сфері інформаційної та кібернетичної безпеки, міжнародним стандартам, а також враховує особливості актуальних кіберзагроз, з якими стикаються державні установи, телекомунікаційні оператори та приватний сектор.

Аналіз змісту програми показує її чітку практичну орієнтованість. Вважаємо, що навчання згідно даної програми може сформувати компетентності у таких напрямках:

- захист інформаційних та інформаційно-комунікаційних систем;
- реагування на кіберінциденти та робота в SOC;
- управління ризиками та безперервністю бізнес-процесів;
- криптографічний та технічний захист інформації;
- мережеві технології безпеки;
- застосування міжнародних стандартів та нормативно-правової бази.

Важливою перевагою програми є наявність лабораторної бази, що моделює реальне середовище кіберзахисту (SIEM-системи, засоби захисту кінцевих точок, мережеві рішення, засоби аналізу інцидентів). Це забезпечує підготовку студентів до виконання професійних функцій без додаткового тривалого навчання на підприємстві.

Позитивно оцінюємо:

- залучення фахівців-практиків до освітнього процесу;
- проходження практик у партнерських організаціях;
- викладання частини дисциплін англійською мовою;
- формування компетентностей реагування на інциденти та аналізу загроз, що є найбільш затребуваними на ринку праці.

Програмні результати навчання знаходимо такими, що відповідають типовим посадовим ролям: junior SOC analyst, фахівець з реагування на інциденти, адміністратор безпеки, спеціаліст з захисту інформації, спеціаліст з підтримки інфраструктури кіберзахисту.

Випускники, підготовлені за даною освітньою програмою, можуть бути ефективно залучені до роботи в компаніях-інтеграторах, центрах кіберзахисту, телекомунікаційних операторах, державних установах та IT-організаціях без необхідності тривалої адаптації.

ТОВ "Центр інформаційної та технічної підтримки "САПФОРІС", що є ексклюзивним партнером та має право здійснювати технічне супроводження продуктів ESET в Україні, може зробити наступний висновок:

Освітня програма «Інформаційна та кібернетична безпека» відповідає сучасним вимогам галузі кібербезпеки, враховує потреби роботодавців та може бути рекомендована до впровадження в освітній процес.

Директор ТОВ «Центр інформаційної та технічної підтримки «Сапфоріс»



Олександр ІЛЛЮША

РЕЦЕНЗІЯ

на освітньо-професійну програму
«Інформаційна та кібернетична безпека»
першого (бакалаврського) рівня вищої освіти
за спеціальністю F5 «Кібербезпека та захист інформації»
Державного університету інформаційно-комунікаційних технологій

Освітньо-професійна програма «Інформаційна та кібернетична безпека» є логічно структурованою та відповідає вимогам стандарту вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації» першого (бакалаврського) рівня.

Мета програми, сформульовані інтегральні, загальні та фахові компетентності, а також програмні результати навчання узгоджені між собою та забезпечують досягнення заявлених результатів підготовки фахівця у сфері кібербезпеки. Простежується коректна відповідність між освітніми компонентами, компетентностями та результатами навчання, що свідчить про системний підхід до проектування освітнього процесу.

Структура освітньої програми збалансовано поєднує фундаментальну підготовку (математика, теорія інформації, фізика, програмування) з професійно орієнтованими дисциплінами (криптографія, мережна безпека, аналіз уразливостей, цифрова криміналістика, системи управління інформаційною безпекою). Значна увага приділяється формуванню компетентностей у сфері управління ризиками, безперервності бізнес-процесів та реагування на кіберінциденти.

Позитивною особливістю програми є:

- наявність практичної підготовки на всіх етапах навчання;
- інтеграція сучасних технологій кіберзахисту в освітній процес;
- викладання окремих дисциплін англійською мовою;
- орієнтація на міжнародні стандарти та практики кібербезпеки;
- можливість академічної мобільності та подальшого навчання на другому рівні вищої освіти.

Зміст програми відповідає сучасним науковим підходам у галузі інформаційної безпеки та може бути співвіднесений з аналогічними освітніми програмами європейського простору вищої освіти. Передбачені форми атестації забезпечують об'єктивну перевірку досягнення результатів навчання.

Висновок:

Освітньо-професійна програма «Інформаційна та кібернетична безпека» є актуальною, методично обґрунтованою та відповідає вимогам підготовки бакалаврів у галузі інформаційних технологій. Програма може бути рекомендована до впровадження та подальшого розвитку.

В.о. завідувач кафедри кібербезпеки
та комп'ютерної інженерії
Київського національного університету
будівництва та архітектури

Максим ДЕЛЕМБОВСЬКИЙ

Підпис: *Делембовський М.М. завідувач*
Секретар: *В.В. Кнуш*
М.О. Климченко

