МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ЗАТВЕРДЖЕНО

Протокол № _____
від "_____"_____2025 р.

засідання вченої ради НУБіП України

Ректор_____ Вадим ТКАЧУК

Освітньо-професійна програма вводиться в дію

з _____2025 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Кібербезпека»

підготовки здобувачів вищої освіти

першого (бакалаврського) рівня вищої освіти

за спеціальністю F5 «Кібербезпека та захист інформації»
код найменування

галузі знань F «Інформаційні технології»
шифр найменування

Кваліфікація: Бакалавр з кібербезпеки та захисту інформації

Стандарт вищої освіти затверджено наказом МОН України від «29» жовтня 2024 р. № 1547

Київ – 2025

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

Проректор з науково-педагогічної

роботи та цифрової трансформації _____ Олена ГЛАЗУНОВА

Керівник центру забезпечення якості освіти____ Ярослав РУДИК

Начальник навчального відділу _____ Оксана ЗАЗИМКО

Декан факультету (директор ННІ) _____ Ігор Болбот

Гарант програми _____ Валерій Лахно

ПЕРЕДМОВА

Освітньо-професійна програма (ОПП) для підготовки здобувачів вищої освіти першого (бакалаврського) рівня за спеціальністю F5 **«**Кібербезпека та захист інформації**»** містить обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти; перелік компетентностей випускника, нормативний зміст підготовки здобувачів вищої освіти, сформульований в термінах результатів навчання; форми атестації здобувачів вищої освіти; вимоги до наявності системи внутрішнього забезпечення якості вищої освіти.

Розроблено проектною групою у складі:

1. Лахно Валерій Анатолійович, доктор технічних наук, професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки, гарант програми;

2. Мамченко Сергій Миколайович, д.п.н., професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки;

3. Сагун Андрій Вікторович, к.т.н., доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки;

4. Кулініч Олег Миколайович, к.т.н., доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки;

5. Фоміна Арина Сергіївна, здобувач вищої освіти ОС «Бакалавр», ОПП Кібербезпека».

Рецензії-відгуки зовнішніх стейкголдерів:

1. Рецензію на освітню програму першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації» надав д.т.н., професор Карпінський М.П., завідувач кафедри інформатики та автоматики, уповноважений ректора до справ Східної Європи університету у Більсько-Бяла (Польща).

2. Рецензію на освітню програму першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації» надав керівник ТОВ «БІОТЕХ ЛТД» Бикін А.В.

3. Рецензію на освітню програму першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації» надав керівник департаменту ТОВ «ITBIZ» Чорноус С.М.

4. Рецензію на освітню програму першого (бакалаврського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації» надав Звєрєв В.П. заступник керівника служби з питань інформаційної безпеки та кібербезпеки, директор центру кіберінтелекту та інновацій у сфері безпеки, керівник управління інформаційної безпеки Апарату Ради Національної безпеки і оборони України, кандидат технічних наук, старший науковий співробітник.

1. Профіль освітньо-професійної програми «Кібербезпека» зі спеціальності F5 «Кібербезпека та захист інформації»

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Національний університет біоресурсів і природокористування України Факультет інформаційних технологій, кафедра комп'ютерних систем, мереж та кібербезпеки
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр. Бакалавр з кібербезпеки та захисту інформації
Офіційна назва освітньо-професійної програми	Кібербезпека
Тип диплому та обсяг освітньо-професійної програми	Диплом бакалавра, одиничний 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців
Наявність акредитації	Сертифікат про акредитацію освітньої програми № 4086 від 22.03.2023 .Строк дії сертифіката до 01.07.2028 р.
Цикл/рівень	НРК України – 6 рівень, FQ -EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Умови вступу визначаються «Правилами прийому до Національного університету біоресурсів і природокористування України», затвердженими Вченою радою. Наявність повної загальної середньої освіти. Підготовка фахівців з кібербезпеки та захисту інформації проводиться за денною формою навчання.
Мова(и) викладання	Українська
Термін дії освітньо-професійної програми	Термін дії освітньо-професійної програми «Кібербезпека» до 2028 року.
Інтернет-адреса постійного розміщення опису освітньо-професійної програми	https://nubip.edu.ua/node/46601
2 – Мета освітньо-професійної програми	
Метою освітньо-професійної програми є формування у майбутнього фахівця здатності динамічно поєднувати знання, уміння, комунікативні навички та спроможності з автономною діяльністю та відповідальністю під час вирішення завдань та проблемних питань в галузі інформаційної та кібернетичної безпеки; забезпечення якісної теоретичної та практичної підготовки у вигляді знань, умінь та навичок за спеціальністю F5 «Кібербезпека та захист інформації» для організації та забезпечення кібернетичної безпеки на об'єктах інформаційної діяльності, зокрема, в галузі АПК.	
3 – Характеристика освітньо-професійної програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	Галузь знань F Інформаційні технології Спеціальність F5 «Кібербезпека та захист інформації». **Об'єкти вивчення:** - 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, зокрема у АПК. **Теоретичний зміст предметної області:** Принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікаційного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. **Методи, методики та технології:** методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації. **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).
Орієнтація освітньо-професійної програми	Освітньо-професійна
Основний фокус освітньо-професійної програми та спеціалізації	Спеціальна в галузі F «Інформаційні технології», спеціальність F5 «Кібербезпека та захист інформації» **Ключові слова:** інформаційно-комунікаційні системи, кібербезпека, захист інформації в комп'ютерних системах та мережах.
Особливості освітньо-професійної програми	Інтегрована підготовка фахівців до створення та використання апаратного і системного програмного забезпечення комп'ютерних систем інформаційної безпеки, кібербезпеки та захисту інформації. З метою підготовки до роботи в реальному середовищі майбутньої професійної діяльності та отримання випускниками освітньої кваліфікації бакалавр з кібербезпеки та захисту інформації програма передбачає надання здобувачам ВО: - системних теоретичних знань в галузі ІТ технологій із поглибленим вивченням спеціалізації безпека інформаційних і комунікаційних систем та мереж; - сучасних компетентностей та практичних навичок з програмування, розробки та управління базами даних, формування моделей захисту інформації та політик безпеки, технічного і криптографічного захисту інформації, побудови захищених IP і TCP мереж та обслуговування сертифікатів відкритих ключів, побудови комплексних систем захисту інформації (далі – КСЗІ) на об'єктах інформаційної діяльності та захисту автоматизованих систем від несанкціонованого доступу, тестування систем захисту інформаційно-комунікаційних систем (далі – ІКС) на проникнення, реалізації управління інформаційною та

	кібернетичною безпекою, адміністрування захищених ІКС, проведення їх моніторингу та аудиту тощо. З метою передачі передового досвіду майбутньому фахівцю, висвітлення в навчальному процесі останніх досягнень науки і техніки, правил ведення успішного бізнесу програма передбачає: - реалізацію процесного підходу при конструюванні змісту профільно-орієнтованих навчальних дисциплін, студентської мобільності, академічної співпраці та молодіжних обмінів; - залучення до викладацької діяльності керівників та професіоналів, які працюють як в системі професійної освіти, так й на виробництві в галузі інформаційних технологій та телекомунікацій, а також представників бізнесу.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Згідно з чинною редакцією Національного класифікатора України: Класифікатор професій (ДК 003:2010, із змінами і доповненнями, внесеними наказами Міністерства економіки України від 16 січня 2024 року N 1410, від 13 грудня 2024 року N 27751) та International Standard Classification of Occupations 2008 (ISCO-08) випускник з професійною кваліфікацією Адміністратор безпеки мереж і систем, Фахівець сфери захисту інформації, Фахівець з питань безпеки (інформаційно-комунікаційні технології), Конструктор систем кібербезпеки, Фахівець з підтримки інфраструктури кіберзахисту, Фахівець з реагування на інциденти кібербезпеки, Фахівець з технічного захисту інформації, Фахівець з тестування систем захисту інформації, Аудитор інформаційних технологій (з кібербезпеки), Фахівець з оцінки заходів захисту інформації (кібербезпеки) може працевлаштуватися на підприємствах і закладах будь-якої форми власності, які працюють в сфері ІТ-технологій, інформаційно-комунікаційного та телекомунікаційного сектора для виконання робіт з адміністрування ОС сімейств Windows/Linux, мережевого обладнання і технологій TCP/IP, DNS, DHCP, SSL/TLS та інші; застосування засобів антивірусного захисту, програмних, клієнт-серверних та хмарних технологій захисту інформації (систем веб фільтрації, систем запобігання вторгнень, систем захисту пошти від вірусів і спаму, тощо); створення технічної, проектної та експлуатаційної документації ІКС) та систем захисту інформації (СЗІ); налагодження, експлуатації та проведення аналізу системних процесів функціонування мережевих, клієнт-серверних та хмарних технологій; проведення моніторингу несанкціонованої активності в обчислювальних системах; створення, впровадження та експлуатації КСЗІ а також СЗІ в складі інформаційно телекомунікаційних (ІТС) та обчислювальних систем; формування політик та процесів у сфері ІТ безпеки, управління доступом до мережевих ресурсів ІТС та ризиками інформаційної безпеки;

	проведення розслідувань інцидентів та забезпечення аудиту процесів інформаційної безпеки.
Подальше навчання	Можливість здобуття освіти на другому (магістерському) рівні за спеціальністю F5 «Кібербезпека та захист інформації» або іншими спорідненими (суміжними) спеціальностями галузі знань F «Інформаційні технології», що узгоджуються з отриманим дипломом бакалавра. **НРК України – 7, FQ-EHEA – 2 цикл, EQF LLL – 7 рівень.**
5 – Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання, технологія проблемного і диференційованого навчання, технологія інтенсифікації та індивідуалізації навчання, технологія програмованого навчання, використання інформаційних технологій, технологія розвивального навчання, кредитно-трансферна система організації навчання, електронне навчання в системі elearn, самонавчання, навчання на основі досліджень. Викладання проводиться у вигляді: лекції, мультимедійної лекції, інтерактивної лекції, семінарів, практичних занять, лабораторних робіт, самостійного навчання на основі підручників та конспектів, консультації з викладачами, підготовка до ЄДКІ.
Оцінювання	Види контролю: поточний, тематичний, періодичний, підсумковий, самоконтроль. Екзамени, заліки та диференційовані заліки проводяться відповідно до вимог "Положення про екзамени та заліки в Національному університеті біоресурсів і природокористування України" (2023 р). В НУБіП України використовується рейтингова форма контролю після закінчення логічно завершеної частини лекційних та практичних занять (модуля) з певної дисципліни. Її результати враховуються під час виставлення підсумкової оцінки. Рейтингове оцінювання знань студентів не скасовує традиційну систему оцінювання, а існує поряд із нею. Воно робить систему оцінювання більш гнучкою, об’єктивною і сприяє систематичній та активній самостійній роботі студентів протягом всього періоду навчання, забезпечує здорову конкуренцію між студентами у навчанні, сприяє виявленню і розвитку творчих здібностей студентів. Рейтинг студента із засвоєння навчальної дисципліни складається з рейтингу з навчальної роботи – 70 балів та рейтингу з атестації – 30 балів. Таким чином, на оцінювання засвоєння змістових модулів, на які поділяється навчальний матеріал дисципліни, передбачається 70 балів. Рейтингові оцінки із змістових модулів, як і рейтинг з атестації, теж обчислюються за 100-бальною шкалою. Письмові екзамени із співбесідою, здача звітів та захист лабораторних/практичних робіт, рефератів в якості самостійної роботи, проведення дискусій, семінарів та модулів. Підготовка та складання ЄДКІ.
6 – Програмні компетентності	

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 і розуміння професійної діяльності. **ЗК3**. Здатність спілкуватися державною мовою як усно, так і письмово. **ЗК4**. Здатність спілкуватися іноземною мовою. **ЗК5**. Здатність вчитися і оволодівати сучасними знаннями. **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 України. **ЗК7**. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. **ЗК8**. Здатність зберігати та приумножувати 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.
Спеціальні (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 комплексних систем захисту інформації (комплекси нормативно-правових, 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	
Програмні результати навчання (ПРН)	**ПРН1**. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. **ПРН2**. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. **ПРН3.** Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. **ПРН4.** 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. **ПРН5.** 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. **ПРН6.** Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. **ПРН7.** 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. **ПРН8.** 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. **ПРН9.** Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. **ПРН10.** Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. **ПРН11.** Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації. **ПРН12.** Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах

	відповідно до встановленої політики інформаційної безпеки. **ПРН13.** 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. **ПРН14.** Вирішувати задачі управляння 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. **ПРН15.** Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи. **ПРН16.** Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах. **ПРН17.** 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. **ПРН18.** Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. **ПРН19.** Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. **ПРН20.** 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. **ПРН21.** 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 в інформаційних системах. **ПРН**22. Вміти застосовувати знання для розв’язування задач аналізу та синтезу засобів, характерних для систем захисту інформації підприємств АПК.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Всього науково-педагогічних працівників –102, у т.ч.: - академіки, члени-кореспонденти НАН України та НААН України – 1,

	- академіки громадських академій – 2, - доктори наук, професори – 17, - кандидати наук, доценти – 49, - асистенти без наукового ступеня – 35
Матеріально-технічне забезпечення	Матеріально-технічна база факультету інформаційних технологій відповідає сучасним вимогам для забезпечення навчального процесу і виконання службових обов'язків співробітниками структурних підрозділів факультету. На факультеті функціонує 182 робочих місця для студентів обладнаних персональними комп'ютерами. Всі комп'ютери підключені до мережі Інтернет. Комп'ютерна техніка знаходиться в працездатному стані. Середній вік ПК, що експлуатуються, становить 7 років. В окремо обладнаній серверній функціонує 4 фізичних сервери, які обслуговують близько 10 віртуальних серверів, у тому числі загальноуніверситетського призначення. Всі аудиторії обладнані презентаційною технікою, системою оповіщення та IP-камерами відеоспостереження. Розгорнута відкрита Wi-Fi мережа з доступом до мережі Інтернет. У навчальному процесі задіяні лабораторії: Навчальна лабораторія хмарних обчислень, Навчальна лабораторія бізнес-аналітики, Навчальна лабораторія інформаційних технологій та архітектури комп'ютерів, Навчальна лабораторія розробки та впровадження інформаційних систем, Навчальна лабораторія інтелектуальних інформаційних систем і технологій. Навчальна лабораторія технологій програмування, Навчальна лабораторія моделювання та 3Д друку, Навчальна лабораторія моделювання і прогнозування, Навчальна лабораторія вбудованих систем та інтернету речей Навчальна лабораторія проектування цифрових пристроїв, Навчально-наукова лабораторія «Технології штучного інтелекту», Навчальна лабораторія «Академія Cisco», Навчальна лабораторія «Кіберполігон».
Інформаційне та навчально-методичне забезпечення	Віртуальне освітнє середовище НУБіП України об'єднує веб-сайт університету (nubip.edu.ua), що містить інформацію про освітні програми, факультети, ННІ, кафедри, розклад занять, контакти викладачів та іншу інформацію; навчально-інформаційний портал (elearn.nubip.edu.ua), на якому розміщені електронні курси навчальних дисциплін; інформаційну систему «Е-деканат», особистий кабінет студента (my.nubip.edu.ua), а також наукову бібліотеку НУБіП України. Бібліотечний фонд – багатогалузевий, нараховує понад 900 тис. примірників видань, у т.ч. рідкісних, авторефератів та повнотестових дисертацій, більше 50 назв журналів та газет, які доступні в центральній бібліотеці та 5 філіях, 8 абонементах з видачі книг, 7 читальних залах на 527 місць з вільним доступом до мережі Інтернет. Електронні ресурси

	бібліотеки: електронний каталог, цифрова бібліотека (https://dglib.nubip.edu.ua) доступна з мережі Інтернет), яка містить понад 8000 повнотекстових видань; електронна бібліотека (доступна з локальної мережі університету), яка містить більше 9000 повнотекстових видань. Матеріали навчально-методичного забезпечення освітньо-професійної програми викладені на сторінці освітньої програми https://nubip.edu.ua/node/46601. Особливості ОПП «Кібербезпека» полягають у здатності здобувачів ВО ефективно використовувати отримані знання для вирішення завдань аналізу, розробки та впровадження комплексних засобів захисту інформації в агропромисловому комплексі. Це включає в себе вміння проводити аналіз вразливостей інформаційних систем підприємств АПК, розробляти та впроваджувати відповідні стратегії безпеки, а також застосовувати методи синтезу засобів захисту для забезпечення конфіденційності, цілісності та доступності даних на різних етапах діяльності підприємств АПК.
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між НУБіП України та закладами вищої освіти України.
Міжнародна кредитна мобільність	На основі двосторонніх договорів та меморандумів між НУБіП України та закордонними закладами вищої освіти щодо програм подвійних дипломів студенти ОПП мають можливість отримати другий диплом, навчаючись у Поморській академії у Слупську (Польща), Словацькому аграрному університеті (Нітра), Академії бізнесу (Домброва Гурніча, Польща). На основі укладених університетом договорів за програмами академічної мобільності ERASMUS+ здобувачі освітньої програми отримують можливість навчання та стажування у провідних європейських та турецьких університетах: Latvia University of Agriculture, University of Foggia (Італія), Dicle Univercity (Туреччина), Technical University in Zvolen (Словаччина), Wroclaw University of Environmental and Life Sciences (Польща), University de Lille (Франція). Здобувачі за освітньою програмою залучаються до літніх шкіл та навчально-наукових проектів, які виконуються спільно з Вроцлавським природничим університетом (Польща), Університетом прикладних наук Вайнштефан Тріздорф (Німеччина), Словацьким технічним університетом, Краківським педагогічним університетом (Польща), Казахським університетом шляхів сполучення.
Навчання іноземних здобувачів вищої освіти	Навчання іноземних здобувачів вищої освіти проводиться на загальних умовах з додатковою мовною підготовкою на підставі міжнародних договорів України; загальнодержавних програм, договорів, укладених з юридичними та фізичними особами.

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

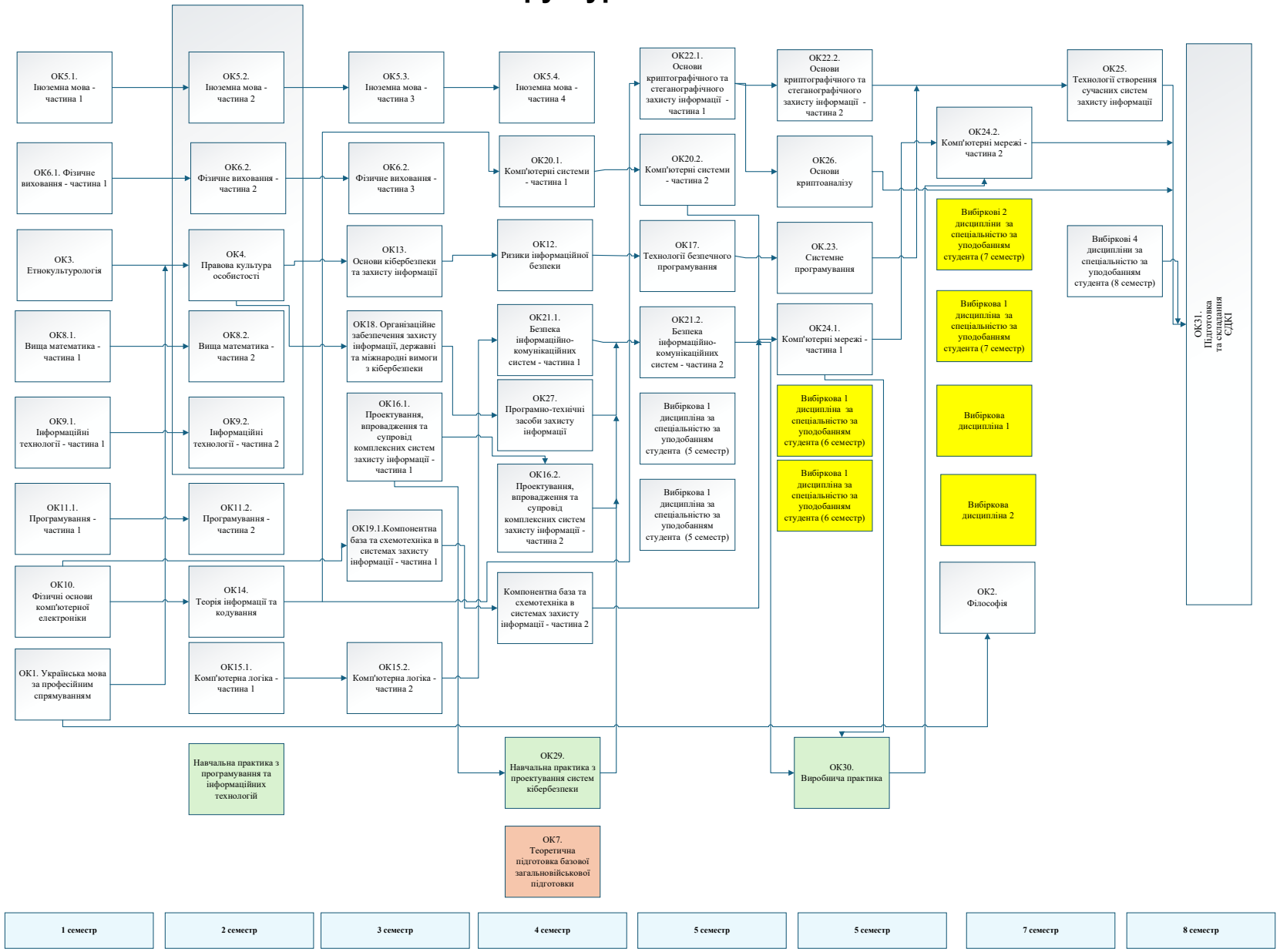
2.1. Перелік компонент ОПП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
1. ОБОВ'ЯЗКОВІ КОМПОНЕНТИ ОПП			
Цикл загальної підготовки			
ОК1	Українська мова за професійним спрямуванням	**3**	**Екзамен**
ОК2	Філософія	**3**	**Екзамен**
ОК3	Етнокультурологія	**3**	**Екзамен**
ОК4	Правова культура особистості	**3**	**Екзамен**
ОК5	Іноземна мова	**8**	**Екзамен**
ОК6	Фізичне виховання	**6**	**Залік**
ОК7	Теоретична підготовка базової загальновійськової підготовки	**3**	**Залік**
Всього:		**29**	
Цикл спеціальної (фахової) підготовки			
ОК8	Вища математика	**10**	**Екзамен**
ОК9	Інформаційні технології	**8**	**Екзамен**
ОК10	Фізичні основи комп'ютерної електроніки	**6**	**Екзамен**
ОК11	Програмування	**8**	**Екзамен**
ОК12	Ризики інформаційної безпеки	**4**	**Екзамен**
ОК13	Основи кібербезпеки та захисту інформації	**4**	**Екзамен**
ОК14	Теорія інформації та кодування	**3**	**Екзамен**
ОК15	Комп'ютерна логіка	**9**	**Екзамен**
ОК16	Проектування, впровадження та супровід комплексних систем захисту інформації	**9**	**Екзамен**
ОК17	Технології безпечного програмування	**5**	**Екзамен**
ОК18	Організаційне забезпечення захисту інформації, державні та міжнародні вимоги з кібербезпеки	**6**	**Екзамен**
ОК19	Компонентна база та схемотехніка в системах захисту інформації	**8**	**Екзамен**
ОК20	Комп'ютерні системи	**8**	**Екзамен**
ОК21	Безпека інформаційно-комунікаційних систем	**8**	**Екзамен**
ОК22	Основи криптографічного та стеганографічного захисту інформації	**8**	**Екзамен**
ОК23	Системне програмування	**5**	**Екзамен**
ОК24	Комп'ютерні мережі	**9**	**Екзамен**
ОК25	Технології створення сучасних систем захисту інформації	**5**	**Екзамен**
ОК26	Основи криптоаналізу	**4**	**Екзамен**
ОК27	Програмно-технічні засоби захисту інформації	**3**	**Екзамен**
	Практична підготовка		
ОК28	Навчальна практика з програмування та інформаційних технологій	**5**	**Залік**
ОК29	Навчальна практика з проектування систем кібербезпеки	**5**	**Залік**
ОК30	Виробнича практика	**5**	**Залік**
	Атестаційний екзамен		

ОК31	Підготовка та складання ЄДКІ (Єдиний державний кваліфікаційний іспит).	**5**	ЄДКІ
Всього:		**150**	
Загальний обсяг обов'язкових компонентів		**179**	
2. ВИБІРКОВІ КОМПОНЕНТИ ОПП			
Цикл загальної підготовки			
ВКУ 1	Вибір з каталогу	3	**Залік**
ВКУ 2	Вибір з каталогу	3	**Залік**
Всього		**6**	
Цикл спеціальної (фахової) підготовки			
Вибіркова 1 дисципліна за спеціальністю за уподобанням студента (5 семестр)			
ВК1.1	Статистичні методи	5	**Залік**
ВК1.2	Техніка і технології в АПК	5	**Залік**
ВК1.3	Типові технологічні об'єкти с.-г. виробництва	5	**Залік**
ВК1.3	Аналітика з R	5	**Залік**
ВК1.4	Комп'ютерна графіка	5	**Залік**
Всього		**5**	
Вибіркова 1 дисципліна за спеціальністю за уподобанням студента (6 семестр)			
ВК2.1	Основи інтернету речей	5	**Екзамен**
ВК2.2	Операційна системи Linux	5	**Екзамен**
ВК2.3	Робототехніка	5	**Екзамен**
ВК2.4	Вебаналітика	5	**Екзамен**
ВК2.5	Безпека життєдіяльності та основи охорони праці	5	**Екзамен**
ВК2.6	Кросплатформне програмування (Python)	**5**	**Екзамен**
Всього		**5**	
Вибіркова 1 дисципліна за спеціальністю за уподобанням студента (5 семестр)			
ВК3.1	Прикладні аспекти побудови систем захисту інформації	5	**Екзамен**
ВК3.2	Основи автоматизованого проєктування	5	**Екзамен**
ВК3.3	Паралельні та розподілені обчислення	5	**Екзамен**
Всього		**5**	
Вибіркова 1 дисципліна за спеціальністю за уподобанням студента (6 семестр)			
ВК4.1	Управління доступом	5	**Екзамен**
ВК4.2	Стандарти інформаційної та кібернетичної безпеки	5	**Екзамен**
ВК4.3	Комп'ютерна електроніка	5	**Екзамен**
ВК4.4	Управління проектами розробки систем захисту інформації	5	**Екзамен**
Всього		**5**	
Вибіркові 2 дисципліни за спеціальністю за уподобанням студента (7 семестр)			
ВК5.1	Проєктування цифрових засобів захисту інформації	5	**Екзамен**
ВК5.2	Оптично волоконні мережі	5	**Екзамен**
ВК5.3	Системне програмне забезпечення	5	**Екзамен**
ВК5.4	Основи аудиту інформаційної безпеки	5	**Екзамен**
Всього		**10**	
Вибіркова 1 дисципліна за спеціальністю за уподобанням студента (7 семестр)			
ВК6.1	Системи моніторингу загроз та атак	5	**Екзамен**
ВК6.2	Крос-платформне програмування	5	**Екзамен**
ВК6.3	Соціальна інженерія	5	**Екзамен**
ВК6.4	3D моделювання і друк	5	**Екзамен**
ВК6.5	Інтелектуальні системи	5	**Екзамен**
ВК6.6	Програмна технологія .NET	5	**Екзамен**
Всього		**5**	

Вибіркові 4 дисципліни за спеціальністю за уподобанням студента (8 семестр)			
ВК7.1	Безпека розробки і підтримки програмних застосунків	5	**Екзамен**
ВК7.2	Проведення розслідувань інцидентів інформаційної безпеки	5	**Екзамен**
ВК7.3	Управління веб-контентом	5	**Екзамен**
ВК7.4	Продукти та послуги інформаційної безпеки	5	**Екзамен**
ВК7.5	Програмування в середовищі сучасних ОС	5	**Екзамен**
ВК7.6	Адміністрування комп'ютерних мереж	5	**Екзамен**
ВК7.7	Машинне навчання	5	**Екзамен**
ВК7.8	Засоби мультимедіа в інформаційних технологіях	5	**Екзамен**
ВК7.9	Програмування мобільних додатків	5	**Екзамен**
ВК7.10	Програмування вбудованих систем	5	**Екзамен**
ВК7.11	Цифрові технології в бізнесі	5	**Екзамен**
Всього		**20**	
Загальний обсяг вибіркових компонентів		**61**	
Разом за ОПП		**240**	

2.2. Структурно-логічна схема



3. Форма атестації здобувачів вищої освіти

Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту. Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом та освітньою програмою та завершується видачею документу встановленого зразка про присудження ступеня бакалавра із присвоєнням кваліфікації: Бакалавр з кібербезпеки та захисту інформації.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми «Кібербезпека»

	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
ЗК 1								+	+	+	+		+	+	+	+	+	+	+	+	+		+	+	+		+	+		+	+
ЗК 2								+	+	+	+	+	+	+		+				+	+				+		+			+	+
ЗК 3	+		+												+	+	+		+	+	+		+								+
ЗК 4					+																										+
ЗК 5								+	+	+	+		+	+	+	+	+		+	+	+		+		+		+				+
ЗК 6			+	+			+						+								+										+
ЗК 7				+									+		+		+		+		+		+								+
ЗК 8		+				+	+						+								+										+
СК 1												+	+			+		+			+								+	+	+
СК 2								+	+	+	+		+	+	+	+	+		+		+		+		+		+		+	+	+
СК 3												+						+			+								+	+	+
СК 4												+				+		+			+			+	+		+		+	+	+
СК 5									+		+					+	+			+	+		+	+	+		+		+	+	+
СК 6																+		+		+	+								+	+	+
СК 7												+				+		+		+	+				+	+	+	+		+	+
СК 8									+		+	+		+								+					+			+	+
СК 9									+		+					+											+			+	+
СК10									+		+		+			+					+	+		+		+		+		+	+

	ВК1.1	ВК1.2	ВК1.3	ВК1.4	ВК1.5	ВК2.1	ВК2.2	ВК2.3	ВК2.4	ВК2.5	ВК2.6	ВК3.1	ВК3.2	ВК3.3	ВК4.1	ВК4.2	ВК4.3	ВК4.4	ВК5.1	ВК5.2	ВК5.3	ВК5.4
ЗК 1	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК 2	+	+		+		+	+	+	+	+		+	+	+	+	+		+	+	+	+	+
ЗК 3												+			+	+	+	+				
ЗК 4												+			+			+				
ЗК 5	+	+			+	+	+	+	+		+	+			+	+	+	+				
ЗК 6		+														+			+	+	+	+
ЗК 7										+						+	+					
ЗК 8										+		+			+			+	+			
СК 1										+		+			+	+		+	+	+	+	+
СК 2	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
СК 3		+	+			+	+	+	+							+						
СК 4		+		+		+	+	+				+			+	+		+	+			
СК 5						+	+	+								+						
СК 6									+			+			+	+		+	+			
СК 7																+						
СК 8					+						+											
СК 9												+							+			+
СК10	+	+				+	+	+		+		+	+	+	+	+		+	+	+	+	+

	ВК6.1	ВК6.2	ВК6.3	ВК6.4	ВК6.5	ВК6.6	ВК7.1	ВК7.2	ВК7.3	ВК7.4	ВК7.5	ВК7.6	ВК7.7	ВК7.8	ВК7.9	ВК7.10	ВК7.11
ЗК 1	+	+	+			+		+			+	+			+	+	+
ЗК 2	+		+	+	+			+	+	+	+		+	+		+	+
ЗК 3			+					+			+						
ЗК 4																	
ЗК 5	+	+	+	+		+		+			+	+		+	+		+
ЗК 6			+					+									+
ЗК 7								+									
ЗК 8			+														
СК 1								+									
СК 2	+	+	+			+		+				+					
СК 3								+				+					
СК 4	+		+									+					
СК 5	+							+	+	+	+	+					
СК 6					+						+						
СК 7	+		+					+			+		+				
СК 8		+															
СК 9																+	
СК10	+							+							+		

5. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньої програми «Кібербезпека»

	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
ПРН1	+												+		+	+	+	+	+	+	+		+				+			+	+
ПРН2					+													+													+
ПРН3							+						+					+			+										+
ПРН4		+						+					+								+			+	+		+		+	+	+
ПРН5						+									+	+	+	+	+	+	+		+		+		+		+	+	+
ПРН6			+						+				+		+	+		+	+	+	+			+						+	+
ПРН7														+		+						+			+	+	+		+	+	+
ПРН8								+		+						+	+			+			+			+				+	+
ПРН9				+								+	+			+		+			+									+	+
ПРН10									+	+	+			+							+				+		+	+	+	+	+
ПРН11									+			+	+			+		+			+								+	+	+
ПРН12										+				+		+		+			+			+	+		+		+	+	+
ПРН13									+		+	+			+	+	+		+	+			+	+	+		+	+		+	+
ПРН14																+					+								+	+	+
ПРН15																					+								+	+	+
ПРН16																+														+	+
ПРН17												+				+					+				+		+			+	+
ПРН18									+		+			+								+						+		+	+
ПРН19										+																+				+	+
ПРН20														+		+								+	+		+			+	+
ПРН21														+		+					+						+		+	+	+
ПРН22															+				+	+	+									+	+

	ВК1.1	ВК1.2	ВК1.3	ВК1.4	ВК1.5	ВК2.1	ВК2.2	ВК2.3	ВК2.4	ВК2.5	ВК2.6	ВК3.1	ВК3.2	ВК3.3	ВК4.1	ВК4.2	ВК4.3	ВК4.4	ВК5.1	ВК5.2	ВК5.3	ВК5.4	ВК6.1	ВК6.2	ВК6.3	ВК6.4	ВК6.5	ВК6.6
ПРН1											+					+	+				+	+		+	+			+
ПРН2																+					+			+				
ПРН3										+						+	+	+				+		+	+			
ПРН4			+			+							+			+		+	+			+	+		+	+		+
ПРН5									+					+		+				+		+	+		+		+	
ПРН6								+					+			+	+			+		+			+	+		+
ПРН7				+				+						+							+		+				+	
ПРН8	+		+				+										+			+						+		
ПРН9									+				+			+				+		+		+				
ПРН10		+	+		+	+					+	+			+				+		+	+	+	+		+	+	+
ПРН11							+							+		+		+	+			+					+	
ПРН12										+		+			+	+			+			+	+					
ПРН13					+						+												+	+				
ПРН14																+						+						
ПРН15																						+			+			
ПРН16																												
ПРН17												+			+	+						+	+		+			
ПРН18											+													+				
ПРН19																+												
ПРН20																						+	+					
ПРН21																						+						
ПРН22			+																					+				

	ВК7.1	ВК7.2	ВК7.3	ВК7.4	ВК7.5	ВК7.6	ВК7.7	ВК7.8	ВК7.9	ВК7.10	ВК7.11
ПРН1		+			+						
ПРН2											
ПРН3		+									
ПРН4	+		+		+	+	+	+	+	+	+
ПРН5		+					+				+
ПРН6		+				+					
ПРН7	+			+	+		+		+	+	
ПРН8							+				+
ПРН9		+		+							
ПРН10	+	+	+	+	+	+	+	+	+	+	
ПРН11		+									+
ПРН12	+	+	+	+				+			+
ПРН13	+				+	+			+	+	
ПРН14		+				+					+
ПРН15		+									
ПРН16											
ПРН17		+		+							+
ПРН18											
ПРН19											
ПРН20											
ПРН21	+	+	+								
ПРН22					+	+					+

6.ЛИСТ ОБЛІКУ ЗМІН ТА ОНОВЛЕННЯ **ОСВІТНЬОЇ ПРОГРАМИ**

Предмет змін	**2025 р.**	**2026 р.**	**2027 р.**
У разі модернізації при зміни законодавства			
Предметна область (галузь знань, спеціальність)	Новий стандарт вищої освіти для спеціальності «Кібербезпека та захист інформації» затверджений наказом МОН України від «29» жовтня 2024 р. № 1547. А також На вимогу Постанови КМУ від 30.08.2024 р. № 1021 «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти» змінено назви галузі та спеціальності ОП.		
Основний фокус освітньої програми	Основний фокус ОПП «Кібербезпека» полягає в здатності здобувачів ВО в ефективно застосовувати знання для аналізу, розробки та впровадження засобів захисту інформації в агропромисловому комплексі, забезпечуючи конфіденційність, цілісність та доступність даних підприємств АПК.		
Компетентності	Згідно стандарту вищої освіти для спеціальності «Кібербезпека та захист інформації» затверджений наказом		

	МОН України від «29» жовтня 2024 р. № 1547.		
Програмні результати навчання	Згідно стандарту вищої освіти для спеціальності «Кібербезпека та захист інформації» затверджений наказом МОН України від «29» жовтня 2024 р. № 1547.		
При плановому оновленні			
Матриці відповідності ЗК, СК, ПРН	Згідно стандарту вищої освіти для спеціальності «Кібербезпека та захист інформації» затверджений наказом МОН України від «29» жовтня 2024 р. № 1547.		
Характеристики інформаційного та навчально-методичного забезпечення	Оновлені відповідно до стандарту вищої освіти для спеціальності «Кібербезпека та захист інформації» затверджений наказом МОН України від «29» жовтня 2024 р. № 1547.		
Структурно-логічна схема	Оновлена відповідно до стандарту вищої освіти для спеціальності «Кібербезпека та захист інформації» затверджений наказом МОН України від «29» жовтня 2024 р. № 1547.		
Перелік освітніх компонентів (дисципліни, практики, курсові роботи/проєкти, кваліфікаційні роботи)	На вимогу статті 101 Закону України «Про військовий обов’язок і військову службу» введено базову загальновійськову підготовку.		

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет інформаційних технологій

НАВЧАЛЬНИЙ ПЛАН
підготовки здобувачів вищої освіти 2025 року вступу

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	F «Інформаційні технології»
Спеціальність	F5 «Кібербезпека та захист інформації»
Освітньо-професійна програма	«Кібербезпека»
Форма здобуття вищої освіти	денна
Термін навчання (обсяг кредитів ЄКТС)	3 роки 10 місяців (240)
На основі	повної загальної середньої освіти
Освітній ступінь	«Бакалавр»
Кваліфікація	_____

І. ГРАФІК ОСВІТНЬОГО ПРОЦЕСУ

підготовки здобувачів освіти першого (бакалаврського) рівня вищої освіти 2025 року вступу

спеціальності F5 «Кібербезпека та захист інформації»

освітньо-професійної програми «Кібербезпека»

Рік навчання	2025 рік																	2026 рік																																		
	Вересень				29	Жовтень			27	Листопад				Грудень				29	Січень				Лютий				Березень				30	Квітень			27	Травень				Червень				29	Липень			27	Серпень			
	1	8	15	22	IX	6	13	20	X	3	10	17	24	1	8	15	22	XII	5	12	19	26	2	9	16	23	2	9	16	23	III	6	13	20	IV	4	11	18	25	1	8	15	22	VI	6	13	20	VII	Сер	Сер	Сер	Сер
					4				1									3													4				2									4				1				
	6	13	20	27	X	11	18	25	XI	8	15	22	29	6	13	20	27	I	10	17	24	31	7	14	21	28	7	14	21	28	IV	11	18	25	V	9	16	23	30	6	13	20	27	VII	11	18	25	VIII	8	15	22	29
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
1								А	А							:	:	-	-	-	-	-								А	А							:	:	:	О	О	О	О	О	О	-	-	-	-	-	-
2								А	А							:	:	-	-	-	-	-								А	А							:	:	:	О	О	О	О	О	О	-	-	-	-	-	-
3								А	А							:	:	-	-	-	-	-								А	А							:	:	:	О	О	О	О	О	О	-	-	-	-	-	-
4								А	А							:	:	-	-	-	-	-								А	А				:	:	:	ІІ	ІІ	ІІ	ІІ	ІІ	//									

Умовні позначення:

	-	теоретичне навчання
:	-	екзаменаційна сесія
-	-	канікули
А	-	
Х	-	виробнича практика
О	-	навчальна практика
ІІ	-	підготовка бакалаврської кваліфікаційної роботи
//		атестація здобувачів вищої освіти (захист бакалаврської кваліфікаційної роботи)

ІІ. ПЛАН НАВЧАЛЬНОГО ПРОЦЕСУ

№ п.п.	Назва навчальної дисципліни	Загальний обсяг		Форми контролю знань (за семестрами)			Аудиторні заняття				Самостійна робота	Практична підготовка		Розподіл тижневих годин за курсами та семестрами							
								у тому числі						I курс		II курс		III курс		IV курс	
														Семестри							
														1	2	3	4	5	6	7	8
														Кількість тижнів у семестрі							
		Годин	(1ЄСТС 30 год). кредитів	Екзамен	Залік	Курсова робота (проект)	Всього	лекції	лабораторні	практичні		Навч. практика	Виробн. практика	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**12**
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1. ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ																					
1.1 Обов'язкові компоненти ОПП																					
ОК1	Українська мова за професійним спрямуванням	90	3	1			30			30	60			2							
ОК2	Філософія	90	3	7			45	15		30	45									3	
ОК3	Етнокультурологія	90	3	1			30	15		15	60			2							
ОК4	Правова культура особистості	90	3	2			30	15		15	60				2						
ОК5.1	Іноземна мова - частина 1	60	2		1		30			30	30			2							
ОК5.2	Іноземна мова - частина 2	60	2	2			30			30	30				2						
ОК5.3	Іноземна мова - частина 3	60	2		3		30			30	30					2					
ОК5.4	Іноземна мова - частина 4	60	2	4			30			30	30						2				
ОК6.1	Фізичне виховання - частина 1	60	2		1		30			30	30			2							
ОК6.2	Фізичне виховання - частина 2	30	1		2		30			30					2						
ОК6.3	Фізичне виховання - частина 3	90	3		3		30			30	60					2					
ОК7	Теоретична підготовка базової загальновійськової підготовки	90	3		4		62	38		24	28						4				
Всього		**870**	**29**	**17**	**6**		**407**	**83**		**324**	**463**			**8**	**6**	**4**	**6**			**3**	
1.3 Вибіркові компоненти ОПП																					
Вибіркова 1 дисципліна за спеціальністю за уподобанням студента (5 семестр)																					
ВК1.1	Статистичні методи	150	5		5		60	30		30	90							4			
ВК1.2	Техніка і технології в АПК	150	5		5		60	30		30	90							4			
ВК1.3	Типові технологічні об'єкти с.-г.виробництва	150	5		5		60	30		30	90							4			

ВК1.3	Аналітика з R	150	5		5		60	30		30	90							4			
ВК1.4	Комп'ютерна графіка	150	5		5		60	30		30	90							4			
ВК1.5	Кросплатформне програмування (Java)	150	5		5		60	30		30	90							4			
Всього		**150**	**5**		**1**		**60**	**30**		**30**	**90**							**4**			
Вибіркова 1 дисципліна за спеціальністю за уподобанням студента (6 семестр)																					
ВК2.1	Основи інтернету речей	150	5	6			60	30		30	90								4		
ВК2.2	Операційна системи Linux	150	5	6			60	30		30	90								4		
ВК2.3	Робототехніка	150	5	6			60	30		30	90								4		
ВК2.4	Вебаналітика	150	5	6			60	30		30	90								4		
ВК2.5	Безпека життєдіяльності та основи охорони праці	150	5	6			60	30		30	90								4		
ВК2.6	Кросплатформне програмування (Python)	150	5	6			60	30		30	90								4		
Всього		**150**	**5**	**1**			**60**	**30**		**30**	**90**								**4**		
Вибіркові дисципліни за уподобанням студента (7 семестр)																					
ВКУ1	Вибіркова дисципліна 1	90	3		7		30	15		15	60									2	
ВКУ2	Вибіркова дисципліна 2	90	3		7		30	15		15	60									2	
Всього		**180**	**6**		**2**		**60**	**30**		**30**	**120**									**4**	
2. ЦИКЛ СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ																					
2.1 Обов'язкові компоненти ОПП																					
ОК8.1	Вища математика - частина 1	180	6		1		90	30		60	90			6							
ОК8.2	Вища математика - частина 2	120	4	2			75	30		45	45				5						
ОК9.1	Інформаційні технології - частина 1	120	4		1		60	30	30		60			4							
ОК9.2	Інформаційні технології - частина 2	120	4	2			75	30	45		45				5						
ОК10	Фізичні основи комп'ютерної електроніки	180	6	1			120	60	60		60			8							
ОК11.1	Програмування - частина 1	120	4		1		60	30	30		60			4							
ОК11.2	Програмування - частина 2	120	4	2			75	30	45		45				5						
ОК12	Ризики інформаційної безпеки	120	4	4			60	30		30	60						4				
ОК13	Основи кібербезпеки та захисту інформації	120	4	3			45	15	30		75					3					
ОК14	Теорія інформації та кодування	90	3	2			60	30	30		30				4						
ОК15.1	Комп'ютерна логіка - частина 1	120	4		2		75	30	45		45				5						
ОК15.2	Комп'ютерна логіка - частина 2	150	5	3		3,КП	75	30	45		75					5					

ОК16.1	Проектування, впровадження та супровід комплексних систем захисту інформації - частина 1	150	5	3			90	45	45		60					6					
ОК16.2	Проектування, впровадження та супровід комплексних систем захисту інформації - частина 2	120	4	4		4,КП	60	30	30		60						4				
ОК17	Технології безпечного програмування	150	5	5		5,КП	60	30	30		90							4			
ОК18	Організаційне забезпечення захисту інформації, державні та міжнародні вимоги з кібербезпеки	180	6	3			90	30	60		90					6					
ОК19.1	Компонентна база та схемотехніка в системах захисту інформації - частина 1	150	5		3		60	30	30		90					4					
ОК19.2	Компонентна база та схемотехніка в системах захисту інформації - частина 2	90	3	4			60	30	30		30						4				
ОК20.1	Комп'ютерні системи - частина 1	90	3		4		60	30	30		30						4				
ОК20.2	Комп'ютерні системи - частина 2	150	5	5			60	30	30		90							4			
ОК21.1	Безпека інформаційно-комунікаційних систем - частина 1	90	3	4			60	30	30		30						4				
ОК21.2	Безпека інформаційно-комунікаційних систем - частина 2	150	5	5			75	30	45		75							5			
ОК22.1	Основи криптографічного та стеганографічного захисту інформації - частина 1	150	5		5		75	30	45		75							5			
ОК22.2	Основи криптографічного та стеганографічного захисту інформації - частина 2	90	3	6		6,КП	60	30	30		30								4		
ОК23	Системне програмування	150	5	6			90	45	45		60								6		
ОК24.1	Комп'ютерні мережі - частина 1	90	3		6		60	30	30		30								4		
ОК24.2	Комп'ютерні мережі - частина 2	180	6	7		7,КП	75	30	45		105									5	
ОК25	Технології створення сучасних систем захисту інформації	150	5	8			96	48	48		54										8
ОК26	Основи криптоаналізу	120	4	6			60	30	30		60								4		

ОК27	Програмно-технічні засоби захисту інформації	90	3	4			60	30	30		30						4				
ОК28	Навчальна практика з програмування та інформаційних технологій	150	5		2							150									
ОК29	Навчальна практика з проектування систем кібербезпеки	150	5		4							150									
ОК30	Виробнича практика	150	5		6							150									
ОК31	Підготовка та складання ЄДКІ	150	5									**150**									
Всього		**4500**	**150**	**22**	**11**	**5**	**2121**	**963**	**1023**	**135**	**1779**	**600**		**22**	**24**	**24**	**24**	**18**	**18**	**5**	**8**
Загальний обсяг обов'язкових компонентів		**5370**	**179**	**39**	**17**	**5**	**2528**	**1046**	**1023**	**459**	**2242**	**600**		**30**	**30**	**28**	**30**	**18**	**18**	**8**	**8**
2.3 Вибіркові компоненти ОПП																					
Вибіркова 1 дисципліна за спеціальністю за уподобанням студента (5 семестр)																					
ВК3.1	Прикладні аспекти побудови систем захисту інформації	150	5	5			60	30	30		90							4			
ВК3.2	Основи автоматизованого проєктування	150	5	5			60	30	30		90							4			
ВК3.3	Паралельні та розподілені обчислення	150	5	5			60	30	30		90							4			
Всього		**150**	**5**	**1**			**60**	**30**	**30**		**90**							**4**			
Вибіркова 1 дисципліна за спеціальністю за уподобанням студента (6 семестр)																					
ВК4.1	Управління доступом	150	5	6			60	30	30		90								4		
ВК4.2	Стандарти інформаційної та кібернетичної безпеки	150	5	6			60	30	30		90								4		
ВК4.3	Комп'ютерна електроніка	150	5	6			60	30	30		90								4		
ВК4.4	Управління проектами розробки систем захисту інформації	150	5	6			60	30	30		90								4		
Всього		**150**	**5**	**1**			**60**	**30**	**30**		**90**								**4**		
Вибіркові 2 дисципліни за спеціальністю за уподобанням студента (7 семестр)																					
ВК5.1	Проєктування цифрових засобів захисту інформації	150	5	7			60	30	30		90									4	
ВК5.2	Оптично волоконні мережі	150	5	7			60	30	30		90									4	
ВК5.3	Системне програмне забезпечення	150	5	7			60	30	30		90									4	
ВК5.4	Основи аудиту інформаційної безпеки	150	5	7			60	30	30		90									4	
Всього		**300**	**10**	**2**			**120**	**60**	**60**		**180**									**8**	
Вибіркова 1 дисципліна за спеціальністю за уподобанням студента (7 семестр)																					
ВК6.1	Системи моніторингу загроз та атак	150	5	7			60	30	30		90									4	
ВК6.2	Крос-платформне програмування	150	5	7			60	30	30		90									4	

ВК6.3	Соціальна інженерія	150	5	7			60	30	30		90								4		
ВК6.4	3D моделювання і друк	150	5	7			60	30	30		90								4		
ВК6.5	Інтелектуальні системи	150	5	7			60	30	30		90								4		
ВК6.6	Програмна технологія .NET	150	5	7			60	30	30		90								4		
Всього		**150**	**5**	**1**			**60**	**30**	**30**		**90**								**4**		
Вибіркові 4 дисципліни за спеціальністю за уподобанням студента (8 семестр)																					
ВК7.1	Безпека розробки і підтримки програмних застосунків	150	5	8			48	24	24		102										4
ВК7.2	Проведення розслідувань інцидентів інформаційної безпеки	150	5	8			48	24	24		102										4
ВК7.3	Управління веб-контентом	150	5	8			48	24	24		102										4
ВК7.4	Продукти та послуги інформаційної безпеки	150	5	8			48	24	24		102										4
ВК7.5	Програмування в середовищі сучасних ОС	150	5	8			48	24	24		102										4
ВК7.6	Адміністрування комп'ютерних мереж	150	5	8			48	24	24		102										4
ВК7.7	Машинне навчання	150	5	8			48	24	24		102										4
ВК7.8	Засоби мультимедіа в інформаційних технологіях	150	5	8			48	24	24		102										4
ВК7.9	Програмування мобільних додатків	150	5	8			48	24	24		102										4
ВК7.10	Програмування вбудованих систем	150	5	8			48	24	24		102										4
ВК7.11	Цифрові технології в бізнесі	150	5	8			48	24	24		102										4
Всього		**600**	**20**	**4**			**192**	**96**	**96**		**408**										**16**
Загальний обсяг вибіркових компонентів		**1830**	**61**	**10**	**3**		**672**	**336**	**246**	**90**	**1158**							**8**	**8**	**16**	**16**
Кількість екзаменів					**49**									3	6	4	6	4	5	5	5
Кількість заліків					**20**									5	3	3	3	2	2	2	
Кількість курсових проектів і робіт					**5**											1	1	1	1	1	
Всього годин навчальних занять		**7200**	**240**	**49**	**20**	**5**	**3200**	**1382**	**1269**	**549**	**3400**	**600**		**30**	**30**	**28**	**30**	**26**	**26**	**24**	**24**

III. СТРУКТУРА НАВЧАЛЬНОГО ПЛАНУ

Навчальні дисципліни	Години	Кредити	%
1. Обов'язкові компоненти ОПП	**5370**	**179**	**74,6**
2. Вибіркові компоненти ОПП	**1830**	**61**	**25,4**
Вибіркові дисципліни за спеціальністю	**1650**	**55**	**22,9**
Вибіркові дисципліни за уподобанням студента	**180**	**6**	**2,5**
3. Інші види навчання			

IV. ЗВЕДЕНІ ДАНІ ПРО БЮДЖЕТ ЧАСУ, ТИЖНІ

Рік навчання	Теоретичне навчання	Екзаменаційна сесія	Практична підготовка	Підготовка бакалаврської роботи	Атестація	Канікули	Всього
1	26	5	6			10	47
2	26	5	6			10	47
3	26	5	0			10	41
4	23	5	0	-1	6	5	38
Разом за ОПП	101	20	12	-1	6	35	173

V. ПРАКТИЧНА ПІДГОТОВКА

№	Вид практики	Семестр	Години	Кредити	Кількість тижнів
1	Навчальна практика з програмування та інформаційних технологій	2	150	5	6
2	Навчальна практика з проектування систем кібербезпеки	4	150	5	6
3	Виробнича практика	6	150	5	0

VI. КУРСОВІ РОБОТИ І ПРОЕКТИ

№	Назва дисципліни	Семестр	Години	Кредити	Курсова робота	Курсовий проект
1	Комп'ютерна логіка	3	30	1		+
2	Проектування, впровадження та супровід комплексних систем захисту інформації	4	30	1		+
3	Технології безпечного програмування	5	15	0,5		+
4	Основи криптографічного та стеганографічного захисту інформації	6	15	0,5		+
5	Комп'ютерні мережі	7	30	1		+

VII. АТЕСТАЦІЯ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

№	Складова атестації	Години	Кредити	Кількість тижнів
1	Підготовка та складання ЄДКІ	150	5	5

Проректор з науково-педагогічної

роботи___ Глазунова О. Г.

Начальник навчального
відділу_____Рудик Я.М.

Декан факультету інформаційних
технологій Болбот І.М.