



**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ**

ЗАТВЕРДЖЕНО

**Протокол №13 від 21 травня 2026 року
засідання вченої ради НУБіП України
Ректор НУБіП України Вадим ТКАЧУК**

**Освітньо-професійна програма
вводиться в дію з 1 вересня 2026 року**

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Кібербезпека»

підготовки здобувачів вищої освіти

першого (бакалаврського) рівня вищої освіти

за спеціальністю F5 «Кібербезпека та захист інформації»

галузі знань F «Інформаційні технології»

Кваліфікація: Бакалавр з кібербезпеки та захисту інформації

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



СЕД НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ Master
№20401 від 01.09.2026. Підписано 01.09.2026. Київ, 03:23:23
Підписав: ТКАЧУК ВАДИМ АНАТОЛІЙОВИЧ
5E984D526F82F38F04000000BFDD2E02A441BF07
Сертифікат діє з 07.07.2026 08:47:36 по 07.07.2027 23:59:59

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. Сагун Андрій Вікторович**, к.т.н., доцент, доцент 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. Лахно Валерій Анатолійович**, д.т.н., професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки;.
- 4. Кулініч Олег Миколайович**, к.т.н., доцент, доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки;.
- 5. Фоміна Арина Сергіївна**, здобувач вищої освіти ОС «Бакалавр», ОПП Кібербезпека».

Рецензії-відгуки зовнішніх стейкхолдерів:

д.т.н., професор Карпінський М.П., уповноважений ректора до справ Східної Європи університету у Більсько-Бяла (Польша)

Зверев 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

Бикін А.В., керівник ТОВ «БІОТЕХ ЛТД»

Чорноус С.М., керівник департаменту ТОВ «ІТВІЗ»

1. Загальна інформація

Повна назва ЗВО та структурного підрозділу: Національний університет біоресурсів і природокористування України, факультет Інформаційних технологій

Ступінь вищої освіти та назва кваліфікації: Бакалавр. Бакалавр з кібербезпеки та захисту інформації

Офіційна назва освітньої програми: Кібербезпека

Тип освітньої програми: Освітньо-професійна

Галузь знань: F «Інформаційні технології»

Обсяг освітньої програми: 240 кредитів

Термін навчання: 3 роки 10 місяців

Форма здобуття освіти: Денна

Мова(и) викладання: Українська

Інтернет-адреса постійного розміщення опису ОП: <https://nubip.edu.ua/node/158423>

Наявність акредитації: Сертифікат про акредитацію освітньої програми №12900 від 28.05.2025. Виданий Національним агентством із забезпечення якості вищої освіти. Строк дії сертифіката до 01.07.2028 р.

2. Мета освітньої 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.

Мета ОПП відповідає Стратегії розвитку НУБіП України "Голосіївська ініціатива".

3. Характеристика програми

Предметна область:

Галузь знань F Інформаційні технології

Спеціальність F5 «Кібербезпека та захист інформації».

Основний фокус програми:

Спеціальна в галузі F «Інформаційні технології», спеціальність F5 «Кібербезпека та захист інформації».

Ключові слова: захист інформації в комп'ютерних системах та мережах, кібербезпека об'єктів апк., інформаційно-комунікаційні системи, кібербезпека

Особливості програми:

Інтегрована підготовка фахівців до створення та використання апаратного і системного програмного забезпечення комп'ютерних систем інформаційної безпеки, кібербезпеки та захисту інформації з врахуванням реалізації Стратегії розвитку НУБіП України "Голосіївська ініціатива".

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

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.

Можливості продовження 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" (Наказ №202 від 28.02.2025 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, підготовки та складання ЄДКІ.

6. Програмні компетентності

Інтегральна компетентність:

Здатність розв'язувати складні спеціалізовані- задачі і практичні завдання у галузі кібербезпеки та захисту інформації, в тому числі – в сфері АПК.

Загальні компетентності:

Код	Компетентність
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 Україні.
ЗК7	Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недобросовісності.

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.
ЗК9	Здатність брати участь у національному спротиві

Спеціальні (фахові) компетентності:

Код	Компетентність
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

Код	Програмний результат навчання
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 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.
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.

ПРН22	Вміти застосовувати знання для розв'язування задач аналізу та синтезу засобів, характерних для систем захисту інформації підприємств АПК.
ПРН23	Надавати допомогу за алгоритмом MARCH, PAWS, у критичних умовах, користуватися сучасними навігаційними системами та засобами зв'язку, виконувати базові дії зі стрілецькою зброєю та розрізняти мінні загрози, застосовувати тактичні навички для захисту та евакуації населення, протидіяти інформаційному впливу ворога, діяти на місцевості з урахуванням загроз БПЛА

8. Ресурсне забезпечення реалізації програми

Кадрове забезпечення:

Всього науково-педагогічних працівників – 104, 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 загально-університетського призначення.

Всі аудиторії обладнані презентаційною технікою, системою оповіщення та ІР-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 абонементів з видачі книг, 7 читальних залах на 527 місць з вільним доступом до мережі Інтернет. Електронні ресурси бібліотеки: електронний каталог, цифрова бібліотека (<https://dglb.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/158423>

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 University (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.

10. Навчання іноземних здобувачів вищої освіти

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.

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.

11. Умови вступу

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.

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

ОБОВ'ЯЗКОВІ КОМПОНЕНТИ ОПП

Цикл загальної підготовки

Код	Назва дисципліни	Кредити ЕКТС	Форма контролю
OK1	Українська мова за професійним спрямуванням	3	Екзамен
OK2	Філософія	3	Екзамен
OK3	Етнокulturологія	3	Екзамен
OK4	Правова культура особистості	3	Екзамен
OK5.1	Іноземна мова - частина 1	2	Залік
OK5.2	Іноземна мова - частина 2	2	Екзамен
OK5.3	Іноземна мова - частина 3	2	Залік
OK5.4	Іноземна мова - частина	2	Екзамен
OK6.1	Фізичне виховання - частина 1	2	Залік
OK6.2	Фізичне виховання - частина 2	1	Залік
OK6.3	Фізичне виховання - частина 3	3	Залік
OK7	Основи національного спротиву	5	Диф. залік

Цикл спеціальної (фахової) підготовки

Код	Назва дисципліни	Кредити ЕКТС	Форма контролю
OK8.1	Вища математика - частина 1	6	Залік
OK8.2	Вища математика - частина 2	4	Екзамен
OK9.1	Інформаційні технології - частина 1	4	Залік
OK9.2	Інформаційні технології - частина 2	4	Екзамен
OK10	Фізичні основи комп'ютерної електроніки	6	Екзамен
OK11.1	Програмування - частина 1	4	Залік
OK11.2	Програмування - частина 2	4	Екзамен
OK12	Ризики інформаційної безпеки	4	Екзамен
OK13	Основи кібербезпеки та захисту інформації	4	Екзамен
OK14	Теорія інформації та кодування	3	Екзамен
OK15.1	Комп'ютерна логіка - частина 1	3	Екзамен
OK15.2	Комп'ютерна логіка - частина 2	5	Залік
OK16.1	Проектування, впровадження та супровід комплексних систем захисту інформації - частина 1	5	Екзамен

OK16.2	Проектування, впровадження та супровід комплексних систем захисту інформації - частина 2	3	Екзамен
OK17	Технології безпечного програмування	5	Екзамен
OK18	Організаційне забезпечення захисту інформації, державно та міжнародні вимоги з кібербезпеки	6	Екзамен
OK19.1	Компонентна база та схемотехніка в системах захисту інформації - частина 1	5	Залік
OK19.2	Компонентна база та схемотехніка в системах захисту інформації - частина 2	3	Екзамен
OK20.1	Комп'ютерні системи - частина 1	3	Залік
OK20.2	Комп'ютерні системи - частина 2	5	Екзамен
OK21.1	Безпека інформаційно-комунікаційних систем - частина 1	3	Екзамен
OK21.2	Безпека інформаційно-комунікаційних систем - частина 2	5	Екзамен
OK22.1	Основи криптографічного та стеганографічного захисту інформації - частина 1	5	Залік
OK22.2	Основи криптографічного та стеганографічного захисту інформації - частина 2	3	Екзамен
OK23	Системне програмування	5	Екзамен
OK24.1	Комп'ютерні мережі - частина 1	3	Залік
OK24.2	Комп'ютерні мережі - частина 2	6	Екзамен
OK25	Технології створення сучасних систем захисту інформації	5	Екзамен
OK26	Основи криптоаналізу	4	Екзамен
OK27	Програмно-технічні засоби захисту інформації	3	Екзамен
OK28	Навчальна практика з програмування та інформаційних технологій	5	Залік
OK29	Навчальна практика з проектування систем кібербезпеки	5	Залік
OK30	Виробнича практика	5	Залік
OK31	Єдиний державний кваліфікаційний іспит	5	Екзамен

ВИБІРКОВІ КОМПОНЕНТИ ОПП

Цикл загальної підготовки

Код	Назва дисципліни	Кредити ЕКТС	Форма контролю
BKY1	Вибір з каталогу	3	Залік
BKY2	Вибір з каталогу	3	Залік

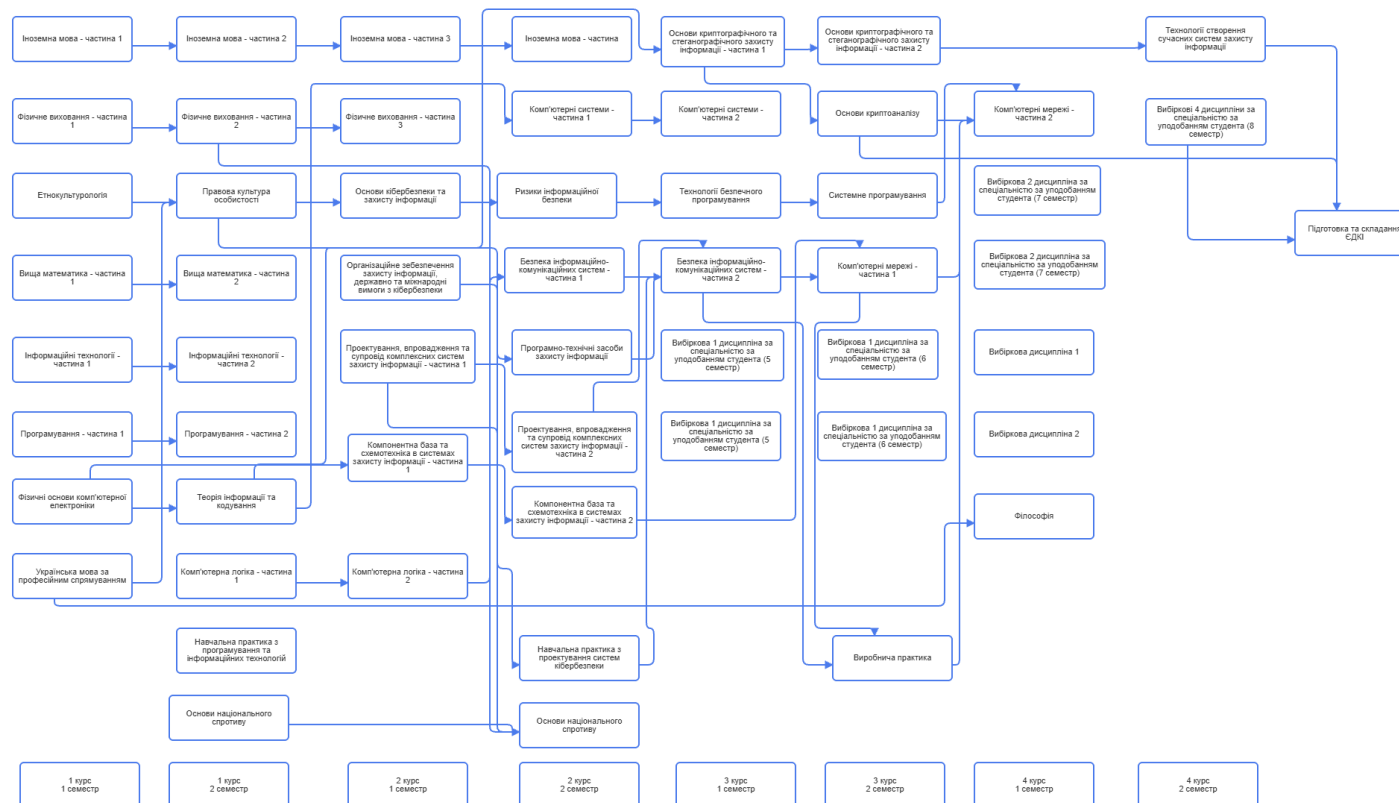
Цикл спеціальної (фахової) підготовки

Код	Назва дисципліни	Кредити ЕКТС	Форма контролю
BK1.1	Статистичні методи	5	Залік
BK1.2	Техніка і технології в АПК-	5	Залік
BK1.3	Типові технологічні об'єкти с.-г виробництва	5	Залік
BK1.4	Аналітика з R	5	Залік

BK1.5	Комп'ютерна графіка	5	Залік
BK1.6	Кросплатформне програмування (Java)	5	Залік
BK2.1	Основи інтернету речей	5	Екзамен
BK2.2	Операційна система Linux	5	Екзамен
BK2.3	Робототехніка	5	Екзамен
BK2.4	Вебаналітика	5	Екзамен
BK2.5	Безпека життєдіяльності та основи охорони праці	5	Екзамен
BK2.6	Кросплатформне програмування (Python)	5	Екзамен
BK3.1	Прикладні аспекти побудови систем захисту інформації	5	Екзамен
BK3.2	Основи автоматизованого проектування	5	Екзамен
BK3.3	Паралельні та розподілені обчислення'	5	Екзамен
BK4.1	Управління доступом	5	Екзамен
BK4.2	Стандарти інформаційної та кібернетичної безпеки	5	Екзамен
BK4.3	Комп'ютерна електроніка	5	Екзамен
BK4.4	Управління проектами розробки систем захисту інформації	5	Екзамен
BK5.1	Проектування цифрових засобів захисту інформації	5	Екзамен
BK5.2	Оптично-волоконні мережі	5	Екзамен
BK5.3	Системне програмне забезпечення	5	Екзамен
BK5.4	Мобільні комп'ютерні системи	5	Екзамен
BK6.1	Системи моніторингу загроз та атак	5	Екзамен
BK6.2	Крос-платформне програмування	5	Екзамен
BK6.3	Соціальна інженерія	5	Екзамен
BK6.4	3D моделювання і друк	5	Екзамен
BK6.5	Інтелектуальні системи	5	Екзамен
BK6.6	Програмне технологія .NET	5	Екзамен
BK7.1	Безпека розробки і підтримки програмних застосунків	5	Екзамен
BK7.2	Проведення розслідування інцидентів інформаційної безпеки	5	Екзамен
BK7.3	Управління веб-контентом	5	Екзамен
BK7.4	Продукти та послуги інформаційної безпеки	5	Екзамен
BK7.5	Програмування в середовищі сучасних ОС	5	Екзамен
BK7.6	Адміністрування комп'ютерних мереж	5	Екзамен
BK7.7	Машинне навчання	5	Екзамен
BK7.8	Засоби мультимедіа в інформаційних технологіях	5	Екзамен
BK7.9	Програмування мобільних додатків	5	Екзамен
BK7.10	Програмування вбудованих систем	5	Екзамен
BK7.11	Цифрові технології в бізнесі	5	Екзамен

Сума обов'язкових компонентів:	179
Сума вибірових компонентів:	61
Всього:	240

Структурно-логічна схема підготовки бакалаврів освітньо-професійної програми «Кібербезпека»



Форма атестації здобувачів вищої освіти

Атестація випускників освітньо-професійної програми «Кібербезпека» спеціальності F5-Кібербезпека та захист інформації здійснюється у формі єдиного державного кваліфікаційного іспиту. Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом та освітньою програмою, та завершується видачею документа встановленого зразка про присудження ступеня бакалавра із присвоєнням кваліфікації:

Бакалавр з кібербезпеки та захисту інформації».

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

Компетентность	OK1	OK2	OK3	OK4	OK5.1	OK5.2	OK5.3	OK5.4	OK6.1	OK6.2	OK6.3	OK7	OK8.1	OK8.2	OK9.1	OK9.2	OK10	OK11.1	OK11.2	OK12	OK13	OK14	OK15.1	OK15.2	OK16.1	OK16.2	OK17	OK18	OK19.1	OK19.2	OK20.1	OK20.2	OK21.1	OK21.2	OK22.1	OK22.2	OK23	OK24.1	OK24.2	OK25	OK26	OK27	OK28	OK29	OK30	OK31	
ЗК1													+	+		+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+				+	+					+	+			
ЗК2													+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+	+					+	+		
ЗК3	+		+																					+	+	+	+	+	+	+	+	+	+	+				+								+	
ЗК4					+	+	+	+																																						+	
ЗК5													+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+			+				+	+			+		
ЗК6			+	+																		+												+	+										+		
ЗК7				+																	+		+	+				+	+	+	+	+	+	+			+								+		
ЗК8		+							+	+	+											+													+	+									+		
ЗК9												+																																			
СК1															+	+				+	+					+	+	+	+	+				+	+									+	+	+	
СК2													+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			+			+	+			+	+	+	
СК3																				+										+				+	+					+				+	+	+	
СК4																				+						+	+	+	+	+				+	+				+	+	+	+			+	+	+
СК5																+	+		+	+					+	+	+	+				+	+	+	+			+	+	+			+	+	+		
СК6																									+	+	+	+				+	+	+	+									+	+	+	
СК7																				+					+	+	+	+	+			+	+	+	+					+	+	+	+			+	+
СК8																+	+	+	+	+		+														+	+					+			+	+	
СК9																+	+	+	+							+	+																+			+	+
СК10																+	+	+	+		+					+	+							+	+	+	+		+	+				+		+	+

Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньо-професійної програми «Кібербезпека»

[illegible]

ЗМІНИ ДО ОСВІТНЬОЇ ПРОГРАМИ

Протокол засідання вченої ради від 26.08.2026 №1

1. У розділ «Загальні компетентності» додано загальну компетентність ЗК9 «Здатність брати участь у національному спротиві» до Компетентності.

2. у розділ «Програмні результати навчання» додано програмний результат навчання ПР15 «Надавати допомогу за алгоритмом MARCH, PAWS у критичних умовах, користуватися сучасними навігаційними системами та засобами зв'язку, виконувати базові дії зі стрілецькою зброєю та розрізняти мінні загрози, застосовувати тактичні навички для захисту та евакуації населення, протидіяти інформаційному впливу ворога, діяти на місцевості із урахуванням загроз БПЛА»;

внесено навчальну дисципліну ОК7 «Основи національного спротиву» (далі – ОНС) до компонентів освітньої програми, матриць відповідності компетентностей та програмних результатів навчання, пов'язавши їх із новою навчальною дисципліною - до Програмні результати навчання.

3. Додано ЗК9 і ПРН23 до Матриці відповідності ЗК, СК, ПРН

4. Зміна назви ОК7 з БЗВП на ОНС в Структурно-логічній схемі

5. На виконання вимог статті 62 Закону України «Про основи національного спротиву», наказу Міністерства освіти і науки України від 30.06.2026 р. № 1002 «Про затвердження Типової програми навчальної дисципліни «Основи національного спротиву», наказу ректора університету від 28.01.2026 р. № 72, з метою організованого викладання дисципліни «Основи національного спротиву» для здобувачів вищої освіти 1 і 2 курсів ступеня бакалавра (магістра ветеринарного спрямування) усіх спеціальностей та відповідно до Наказу ректора №1018 від 16.07.2026 введено викладання обов'язкової навчальної дисципліни «Основи національного спротиву» замість дисципліни "Базова загальна військова підготовки" в обсязі 5 ECTS.

5. Зменшено кількість кредитів ECTS для дисциплін: "Комп'ютерна логіка - частина 1" (до 3 ECTS) та для "Проектування, впровадження та супровід комплексних систем захисту інформації - частина 2" (до 3 ECTS).

6. Тижневе аудиторне навантаження до 2 семестру встановлено 32 години, для 4 семестру - 30 годин.