МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ЗАТВЕРДЖЕНО

ЗАТВЕРДЖЕНО

Протокол № 9 від «28» квітня 2021 р.
засідання вченої ради НУБіП України

Освітньо-професійна програма
вводиться в дію з 1 вересня 2021 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Кібербезпека»

першого (бакалаврського)рівня вищої освіти

за спеціальністю 125 «Кібербезпека»

галузі знань 12 «Інформаційні технології»

Кваліфікація: Бакалавр з кібербезпеки

Стандарт вищої освіти затверджено
наказом МОН України від «04» жовтня 2018 р. № 1074

Київ – 2021

ПЕРЕДМОВА

Освітньо-професійна програма (ОПП) для підготовки здобувачів вищої освіти першого (бакалаврського) рівня за спеціальністю **«**Кібербезпека**»** 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, завідувач кафедри комп'ютерних систем і мереж, **гарант програми**.
2. Сагун Андрій Вікторович, кандидат технічних наук, доцент кафедри комп'ютерних систем і мереж.
3. Блозва Андрій Ігорович, кандидат педагогічних наук, доцент кафедри комп'ютерних систем і мереж.

Рецензії-відгуки зовнішніх стейкголдерів:

1. Рецензію на освітню програму першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека» надав заступник директора Департаменту, начальник відділу Адміністрації Державної служби спеціального зв'язку та захисту інформації України Бакалинський О.О.
2. Рецензію на освітню програму першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека» надав д.е.н., доцент Жемойда О.В., директор департаменту багатосторонніх та двосторонніх торговельних угод Міністерства розвитку економіки, торгівлі та сільського господарства України документ СЕД Мінекономіки АСКОД.
3. Рецензію на освітню програму першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека» надав к.т.н., доцент Гулак Г.М., завідувач науково-дослідної лабораторії «Дослідження з питань кібербезпеки» Інституту математичних машин та систем Національної академії наук України.

1. Профіль освітньо-професійної програми «Кібербезпека» зі спеціальності 125 «Кібербезпека»

1 - Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Національний університет біоресурсів і природокористування України Факультет інформаційних технологій, кафедра комп'ютерних систем і мереж
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр. Бакалавр з кібербезпеки 3439 - Фахівець із організації інформаційної безпеки
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців
Наявність акредитації	Впровадження в 2019 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 проводиться за денною і заочною формами навчання.
Мова(и) викладання	Українська
Термін дії освітньої програми	Термін дії освітньо-професійної програми «Кібербезпека» до 2024 року.
Інтернет-адреса постійного розміщення опису освітньої 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 125 «Кібербезпека» для організації та забезпечення кібернетичної безпеки на об'єктах інформаційної діяльності, зокрема, в галузі АПК.	
3 - Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	Галузь знань 12 Інформаційні технології Спеціальність 125 Кібербезпека. Об'єкти професійної діяльності випускників: - об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; - технології забезпечення безпеки інформації; - процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. Цілі навчання: підготовка фахівців, здатних використовувати і впроваджувати технології

	інформаційної та/або кібербезпеки. Теоретичний зміст предметної області. Знання: - законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; - принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; - теорії, моделей та принципів управління доступом до інформаційних ресурсів; - теорії систем управління інформаційною та/або кібербезпекою; - методів та засобів виявлення, управління та ідентифікації ризиків; - методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; - методів та засобів технічного та криптографічного захисту інформації; - сучасних інформаційно-комунікаційних технологій; - сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; - автоматизованих систем проектування. Методи, методики та технології: методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки. Інструменти та обладнання: - системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; - сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньої програми	Освітньо-професійна
Основний фокус освітньої програми та спеціалізації	Спеціальна в галузі 12 «Інформаційні технології», спеціальність 125 «Кібербезпека» Ключові слова: інформаційна безпека, кібербезпека, захист інформації в комп'ютерних системах.
Особливості програми	Інтегрована підготовка фахівців до створення та використання апаратного і системного програмного забезпечення комп'ютерних систем інформаційної безпеки та кібербезпеки. З метою підготовки до роботи в реальному середовищі майбутньої професійної діяльності та отримання випускниками освітньої кваліфікації бакалавр з кібербезпеки програма передбачає надання студентам: - системних теоретичних знань в галузі IT технологій із поглибленим вивченням спеціалізації безпека інформаційних і комунікаційних систем; - 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) та International Standard Classification of Occupations 2008 (ISCO-08) випускник з професійною кваліфікацією «Фахівець з організації інформаційної безпеки» 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.

	Фахівці, які здобули освіту за освітньою програмою «Кібербезпека», можуть обіймати такі первинні посади: програміст/тестувальник програмного забезпечення систем ІКБ; адміністратор комп'ютерних систем і мереж; адміністратор інформаційної та кібербезпеки; аудитор безпеки інформаційно-комунікаційних систем; розробник засобів захисту інформації; інженер служби технічного захисту інформації, тощо.
Подальше навчання	Можливість здобуття освіти на другому (магістерському) рівні за спеціальністю 125 «Кібербезпека» або іншими спорідненими (суміжними) спеціальностями галузі знань «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 кваліфікаційної роботи бакалавра (проекту).
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" (2019 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 захист дипломного проекту.
	6 – Програмні компетентності
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми в галузі забезпечення інформаційної безпеки та\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (КЗ)	**КЗ 1**. Здатність застосовувати знання у практичних ситуаціях. **КЗ 2**. Знання та розуміння предметної області та розуміння професії. **КЗ 3**. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. **КЗ 4**. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. **КЗ 5**. Здатність до пошуку, оброблення та аналізу інформації. **КЗ 6**. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. **КЗ 7**. 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. **КЗ 8**. Здатність до абстрактного і системного мислення, аналізу та синтезу.
Спеціальні (фахові, предметні) компетентності спеціальності (СК)	**СК1**. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. **СК2**. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. **СК3**. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. **СК4**. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

	СК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. **СК6**. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. **СК7**. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). **СК8**. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. **СК9**. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. **СК10**. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. **СК11**. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. **СК12**. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки. **СК13**. Здатність розробляти апаратне, алгоритмічне та програмне забезпечення, компоненти комп'ютерних систем захисту інформації.
7 - Програмні результати навчання (ПРН)	
	1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

	5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; 12. Розробляти моделі загроз та порушника; 13. Аналізувати проекти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних; 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; 19. Застосовувати теорії, методи та засоби захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в

	інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;

	34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; 36. Виявляти небезпечні сигнали технічних засобів; 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної, і/або кібербезпеки; 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; 44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; 45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних

	системах з використанням сучасних методів та засобів криптографічного захисту інформації; 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; 50. Забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз; 54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. 55. Знати і розуміти наукові, математичні і фізичні положення, що лежать в основі функціонування систем захисту інформації. 56. Вміти застосовувати знання для розв'язування задач аналізу та синтезу засобів, характерних для систем захисту інформації.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Всього науково-педагогічних працівників – 72, у т.ч.: - академіки, члени-кореспонденти НАН України та НААН України – 1, - академіки громадських академій – 8, - доктори наук, професори – 16, - кандидати наук, доценти – 39, - асистенти без наукового ступеня – 17.

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. Вся техніка знаходиться в працездатному стані, середній вік ПК, що експлуатуються, становить 7 років. У навчальному процесі функціонують лабораторії: проектування цифрових пристроїв (розгорнуто стенди Trigger та Logic), моделювання та прогнозування, академія Cisco (серверне та мережеве обладнання), технологій програмування (ліцензійне ПЗ для завдань програмування), лабораторія Microsoft Imagine Academy (онлайн курси та сертифікація за лінійками Майкрософт), IT-компетенцій (базові курси з основ інформаційних технологій), інтелектуальних систем (програмне забезпечення для проектування та розробки інтелектуальних систем), комп'ютерного моніторингу довкілля (дрони Phantom, Mavic, мікрокомп'ютери, датчики, мікросхеми та плати для виготовлення спеціальних комп'ютерів), вбудованих систем та Інтернет речей (стенди з моніторами, плати Arduino, OrangePi, RaspberryPi, конструктори дронів), лабораторія 3D моделювання та друку (моноблоки Apple, 3D принтер), лабораторія «Кіберполігон» (серверне, мережне обладнання), лекційні аудиторії, обладнані мультимедійними проекторами, екранами, IP-камерами для системи відео спостереження. У підрозділах факультету функціонує 207 робочих місця, обладнаних персональними комп'ютерами, у тому числі 203 у комп'ютерних класах, 4 фізичних сервери та 2 сервери типу «Лезо» (Blade), які обслуговують 30 віртуальних серверів, у тому числі понад 12 – загально університетського призначення.
Інформаційне та навчально-методичне забезпечення	Офіційний веб-сайт https://nubip.edu.ua містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти. Всі зареєстровані в університеті користувачі мають необмежений доступ до мережі Інтернет. Матеріали навчально-методичного забезпечення освітньо-професійної програми викладені на освітньому порталі «Навчальна робота»: https://nubip.edu.ua/node/46601. Бібліотечний фонд багатогалузевий, нараховує понад один мільйон примірників вітчизняної та зарубіжної літератури, у т.ч. рідкісних видань, спеціальних видів науково-технічної літератури, авторефератів дисертацій (з 1950 р.), дисертацій (з 1946 р.), більше 500 найменувань журналів та більше 50 назв газет. Фонд комплектується

	матеріалами з сільського та лісового господарства, економіки, техніки та суміжних наук. Бібліотечне обслуговування читачів проводиться на 8 абонементах, у 7 читальних залах на 527 місць, з яких: 4 галузеві, 1 універсальний та 1 спеціалізований читальний зал для викладачів, аспірантів та магістрів (Reference Room); МБА; каталоги, в т.ч. електронний (понад 206292 одиниць записів); бібліографічні картотеки (з 1954 р.); фонд довідкових і бібліографічних видань. Щорічно бібліотека обслуговує понад 40000 користувачів, у т.ч. 14000 студентів. Книговидача становить понад 1 млн примірників на рік. Читальні зали забезпечені бездротовим доступом до мережі Інтернет. Всі ресурси бібліотеки доступні через сайт університету: https://nubip.edu.ua. Цифрова бібліотека НУБіП України була створена у листопаді 2019 р., доступна з мережі Інтернет та містить зараз 790 повнотекстових документи, серед них: 150 навчальних підручників та посібників; 117 монографій; 420 авторефератів дисертацій; 98 оцифрованих рідкісних та цінних видань з фондів бібліотеки (1795-1932 рр.). Важливим електронним ресурсом також є електронна бібліотека (з локальної мережі університету), де є понад 6409 повнотекстових документів (підручників, навчальних посібників, монографій, методичних рекомендацій). З січня 2017 р. в НУБіП України відкрито доступ до однієї із найбільших наукометричних баз даних Web of Science. З листопада 2017 року в НУБіП України відкрито доступ до наукометричної та універсальної реферативної бази даних SCOPUS видавництва Elsevier. Доступ здійснюється з локальної мережі університету за посиланням https://www.scopus.com. База даних SCOPUS індексує близько 22000 назв різних видань (серед яких 55 українських) від більш ніж 5000 видавництв. Матеріали навчально-методичного забезпечення освітньо-професійної програми викладені на навчально-інформаційному порталі НУБіП України http://elearn.nubip.edu.ua. Центр дистанційних технологій навчання проводить підтримку викладачів університету по створенню електронних навчальних курсів на базі LMS Moodle, на якій працює навчально-інформаційний портал https://elearn.nubip.edu.ua. Для забезпечення освітньої програми створено електронні курси до усіх навчальних дисциплін. Кожний електронний навчальний курс містить лекційні матеріали у форматі презентацій, повнотекстових матеріалів, електронних посібників, посилань на он-лайн курси академій Microsoft та Cisco; завдання та методичні рекомендації до виконання лабораторних і проектних

	робіт з посиланнями на платформи і сервіси для практичної роботи (Azure, CodePlex, Programmr тощо); завдання для контролю та самоконтролю студентів, модульні та атестаційні завдання.
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 освітньої програми 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+ та MEVLANA, 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.

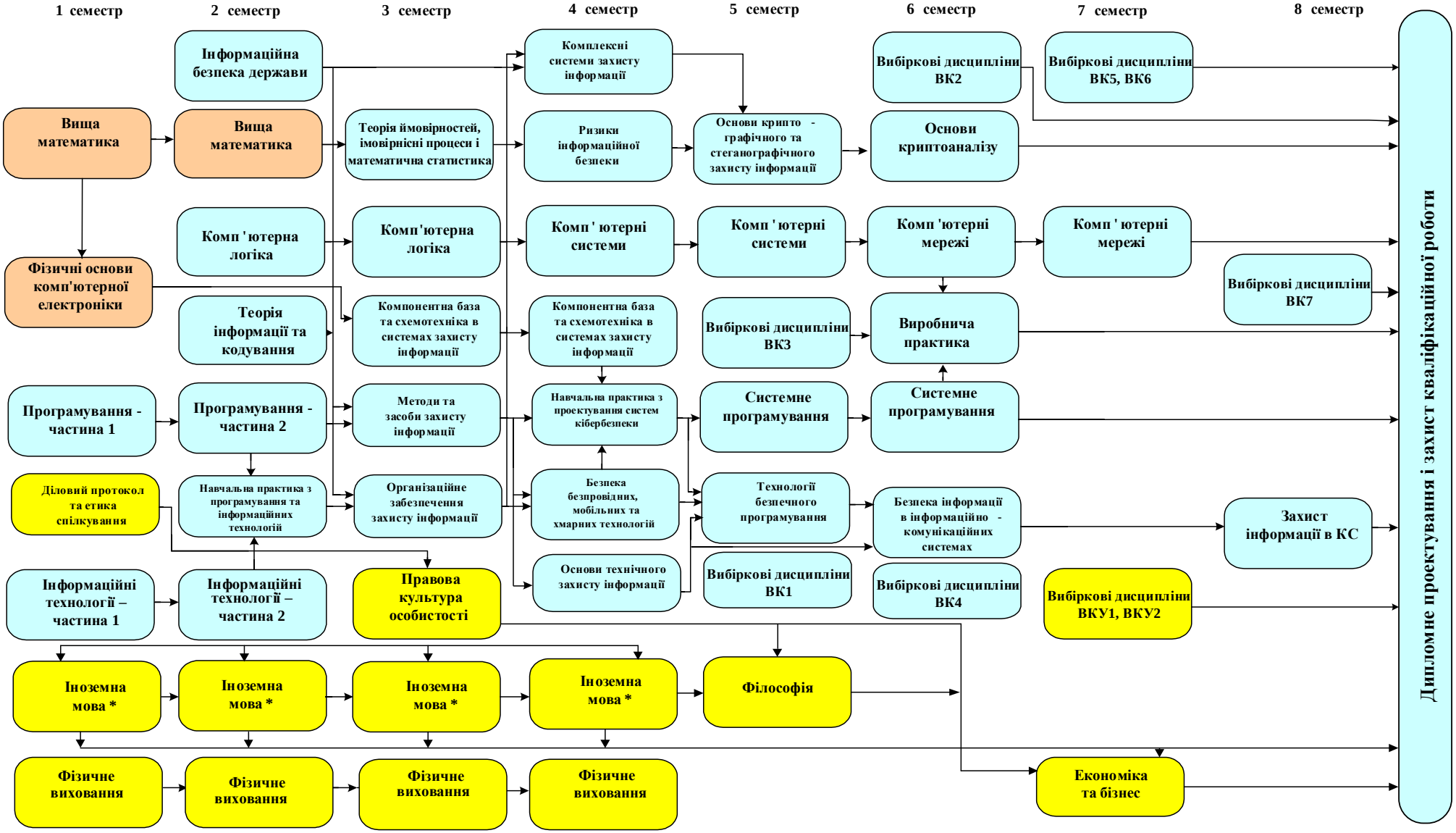
2. Перелік компонент освітньо-професійної програми «Кібербезпека» та їх логічна послідовність

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. ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
Обов'язкові компоненти ОПП			
ОК1	Вища математика	11	екзамен
ОК2	Фізичні основи комп'ютерної електроніки	6	екзамен
ОК3	Програмування	10	екзамен
ОК4	Ризики інформаційної безпеки	4	екзамен
ОК5	Інформаційна безпека держави	4	екзамен
ОК6	Теорія інформації та кодування	4	екзамен
ОК7	Теорія ймовірностей, імовірнісні процеси і математична статистика	4	екзамен
Обов'язкові компоненти ОПП за рекомендацією вченої ради університету			
ОКУ1	Правова культура особистості	4	екзамен
ОКУ2	Діловий протокол та етика спілкування	5	екзамен
ОКУ3	Іноземна мова	8	екзамен
ОКУ4	Філософія	4	екзамен
ОКУ5	Економіка та бізнес	4	екзамен
ОКУ6	Інформаційні технології	8	екзамен
ОКУ7	Фізичне виховання (за рахунок вільного часу студента)	4	залік
Вибіркові компоненти ОПП			
Вибіркова 1 дисципліна за спеціальністю			
ВК1.1	Менеджмент	5	екзамен
ВК1.2	Техніка і технології в АПК	5	екзамен
ВК1.3	Типові технологічні об'єкти с.-г. виробництва	5	екзамен
ВК1.4	Безпека життєдіяльності та основи охорони праці	5	екзамен
Вибіркова 1 дисципліна за спеціальністю			
ВК2.1	Основи інтернету речей	5	екзамен
ВК2.2	Дискретна математика	5	екзамен
ВК2.3	Стандарти інформаційної та кібернетичної безпеки	5	екзамен
ВК2.4	Основи прогнозування та моделювання у соціальній сфері	5	екзамен
Вибіркові дисципліни за уподобанням студента			
ВКУ1	Вибіркова дисципліна 1	4	залік
ВКУ2	Вибіркова дисципліна 2	4	залік
2. ЦИКЛ СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
Обов'язкові компоненти ОПП			
ОК8	Комп'ютерна логіка	8	екзамен
ОК9	Методи та засоби захисту інформації	5	екзамен
ОК10	Комплексні системи захисту інформації	4	екзамен
ОК11	Організаційне забезпечення захисту інформації	5	екзамен
ОК12	Компонентна база та схемотехніка в системах захисту інформації	9	екзамен
ОК13	Комп'ютерні системи	7	екзамен
ОК14	Безпека інформації в інформаційно-комунікаційних системах	4	екзамен
ОК15	Основи криптографічного та стеганографічного	4	екзамен

	захисту інформації		
ОК16	Системне програмування	7	екзамен
ОК17	Комп'ютерні мережі	9	екзамен
ОК18	Безпека безпровідних, мобільних та хмарних технологій	4	екзамен
ОК19	Захист інформації в комп'ютерних системах	5	екзамен
ОК20	Основи криптоаналізу	5	екзамен
ОК21	Основи технічного захисту інформації	4	екзамен
ОК22	Технології безпечного програмування	4	екзамен
ОК23	Навчальна практика з програмування та інформаційних технологій	5	залік
ОК24	Навчальна практика з проектування систем кібербезпеки	5	залік
ОК25	Виробнича (Проектно-технологічна практика)	5	залік
ОК26	Підготовка і захист кваліфікаційної бакалаврської роботи	5	Захист роботи
Загальний обсяг обов'язкових компонентів		**180**	
Вибіркові компоненти ОПП			
Вибіркова 1 дисципліна за спеціальністю за уподобанням студента			
ВК3.1	Прикладні аспекти побудови систем захисту інформації	5	екзамен
ВК3.2	Безпека та аудит безпроводових та рухомих мереж	5	екзамен
ВК3.3	Паралельні та розподілені обчислення	5	екзамен
Вибіркова 1 дисципліна за спеціальністю за уподобанням студента			
ВК4.1	Управління доступом	5	екзамен
ВК4.2	Системний аналіз	5	екзамен
ВК4.3	Комп'ютерна електроніка	5	екзамен
ВК4.4	Управління проектами розробки систем захисту інформації	5	екзамен
Вибіркові 2 дисципліни за спеціальністю за уподобанням студента			
ВК5.1	Ліцензування і сертифікація засобів захисту інформації	4	екзамен
ВК5.2	Безпека при експлуатації і обслуговуванні IT систем	4	екзамен
ВК5.3	Системне програмне забезпечення	4	екзамен
ВК5.4	Основи аудиту інформаційної безпеки	4	екзамен
Вибіркова 1 дисципліна за спеціальністю за уподобанням студента			
ВК6.1	Системи моніторингу загроз та атак	4	екзамен
ВК6.2	Крос-платформне програмування	4	екзамен
ВК6.3	Інформаційно-психологічне протиборство	4	екзамен
Вибіркові 4 дисципліни за спеціальністю за уподобанням студента			
ВК7.1	Безпека розробки і підтримки додатків	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
Загальний обсяг вибіркових компонентів		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОПП		**240**	

2.2. Структурно-логічна схема підготовки фахівців



* - Використовується у багатьох дисциплінах

3. Атестація здобувачів вищої освіти

Атестація випускників освітньої проводиться у формі захисту випускної бакалаврської роботи та завершується видачею документу встановленого зразка про присудження йому ступеня бакалавра із присвоєнням кваліфікації: Бакалавр з кібербезпеки. Атестація здійснюється відкрито і публічно.

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

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОКУ1	ОКУ2	ОКУ3	ОКУ4	ОКУ5	ОКУ6	ОКУ7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17
КЗ 1		+	+	+	+			+	+	+		+	+		+	+	+	+	+	+	+	+	+	+
КЗ 2				+	+											+	+	+	+		+	+		
КЗ 3									+	+														
КЗ 4				+	+											+	+	+	+		+	+		+
КЗ 5					+		+			+	+		+											
КЗ 6					+			+	+		+													
КЗ 7					+			+	+		+	+		+										
КЗ 8	+	+	+	+		+	+				+				+	+	+		+	+		+	+	
СК 1					+			+									+	+				+		
СК 2																+	+				+			+
СК 3																+	+		+	+	+	+	+	+
СК 4												+					+	+						
СК 5				+												+	+	+			+			+
СК 6																		+						
СК 7																+	+	+		+	+			+
СК 8																+		+						
СК 9												+					+	+						
СК10																+	+							
СК11																+								+
СК12																	+							
СК13			+										+				+					+	+	

	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26
К31	+	+	+	+	+	+	+	+	+
К32	+	+	+	+	+	+	+	+	+
К33						+	+	+	+
К34	+	+	+	+		+	+	+	+
К35						+	+	+	+
К36									
К37									
К38		+	+		+		+		+
СК1	+						+	+	+
СК2	+	+			+		+		+
СК3	+	+		+			+	+	+
СК4								+	+
СК5	+	+		+			+		+
СК6	+	+					+	+	+
СК7	+			+			+	+	+
СК8									+
СК9	+						+		+
СК10		+							+
СК11	+			+			+		+
СК12	+	+					+		+
СК13		+			+		+		+

	ВК1.1	ВК1.2	ВК1.3	ВК1.4	ВК2.1	ВК2.2	ВК2.3	ВК2.4	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
КЗ 1	+	+	+		+		+	+	+			+	+		+	+				+		+
КЗ 2		+	+				+		+	+		+	+		+	+	+		+	+		+
КЗ 3	+																					+
КЗ 4									+	+		+	+		+	+	+		+			
КЗ 5	+	+						+					+		+				+			+
КЗ 6				+																		
КЗ 7				+				+														
КЗ 8					+			+		+	+		+	+				+	+	+	+	
СК 1							+								+	+			+			
СК 2					+		+		+	+					+		+					
СК 3			+		+				+			+					+					
СК 4	+																+					
СК 5									+			+					+					
СК 6									+								+			+		
СК 7									+	+							+		+	+		
СК 8										+		+			+	+			+			
СК 9												+			+							
СК10										+							+					
СК11																	+					+
СК12										+									+			+
СК13					+						+			+				+			+	

	ВК7.1	ВК7.2	ВК7.3	ВК7.4	ВК7.5	ВК7.6
КЗ 1			+	+		+
КЗ 2		+	+	+		+
КЗ 3						
КЗ 4	+	+	+	+	+	+
КЗ 5		+				
КЗ 6						
КЗ 7						
КЗ 8		+			+	
СК 1				+		
СК 2				+		+
СК 3	+		+		+	+
СК 4		+	+	+		
СК 5						+
СК 6			+			+
СК 7		+				+
СК 8		+				
СК 9			+			+
СК10	+			+		+
СК11						+
СК12		+				
СК13					+	

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

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОКУ1	ОКУ2	ОКУ3	ОКУ4	ОКУ5	ОКУ6	ОКУ7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17
ПРН1									+	+														
ПРН2												+												
ПРН3			+			+							+		+				+		+	+		
ПРН4															+				+		+	+		
ПРН5													+			+		+						
ПРН6				+							+						+	+			+			
ПРН7					+			+										+						
ПРН8					+													+						
ПРН9					+													+						
ПРН10															+		+			+				
ПРН11																	+							+
ПРН12																+								
ПРН13				+												+	+				+			+
ПРН14																					+		+	+
ПРН15			+										+										+	
ПРН16																	+							
ПРН17																				+	+			+
ПРН18																			+					
ПРН19				+												+						+		
ПРН20																	+				+			
ПРН21																+	+				+			
ПРН22																+	+							
ПРН23																+	+				+			
ПРН24																+	+						+	
ПРН25																+	+	+						
ПРН26																+		+						
ПРН27				+												+								+
ПРН28																+	+	+					+	
ПРН29				+																	+			

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОКУ1	ОКУ2	ОКУ3	ОКУ4	ОКУ5	ОКУ6	ОКУ7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17
ПРН30				+													+				+			
ПРН31				+												+					+			
ПРН32				+														+						
ПРН33				+																				
ПРН34																		+						
ПРН35																	+							
ПРН36																+	+							
ПРН37															+	+	+		+	+				
ПРН38															+	+	+		+	+				
ПРН39																		+						
ПРН40																		+	+					
ПРН41																		+						
ПРН42																		+						
ПРН43				+	+																			
ПРН44				+																				
ПРН45				+													+							
ПРН46				+																				
ПРН47																						+		
ПРН48																						+		
ПРН49																+								
ПРН50																+	+				+			
ПРН51																					+			
ПРН52																					+			
ПРН53																								
ПРН54								+	+															
ПРН55	+	+				+	+																	
ПРН56															+				+	+				

	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26
ПРН1							+		+
ПРН2									+
ПРН3			+			+	+	+	+
ПРН4								+	+
ПРН5				+			+		+
ПРН6		+					+		+
ПРН7							+		+
ПРН8							+		+
ПРН9									+
ПРН10									+
ПРН11	+								+
ПРН12		+					+		+
ПРН13	+			+					+
ПРН14	+	+		+	+				+
ПРН15					+				+
ПРН16									+
ПРН17	+			+					+
ПРН18				+					+
ПРН19		+	+						+
ПРН20								+	+
ПРН21					+		+	+	+
ПРН22				+			+	+	+
ПРН23		+		+			+		+
ПРН24		+		+			+		+
ПРН25	+						+		+
ПРН26							+		+
ПРН27	+								+
ПРН28		+							+
ПРН29		+							+

	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26
ПРН30		+							+
ПРН31		+					+		+
ПРН32				+					+
ПРН33							+		+
ПРН34							+		+
ПРН35							+		+
ПРН36				+					+
ПРН37				+					+
ПРН38				+					+
ПРН39								+	+
ПРН40				+				+	+
ПРН41								+	+
ПРН42								+	+
ПРН43									+
ПРН44								+	+
ПРН45								+	+
ПРН46								+	+
ПРН47			+					+	+
ПРН48			+						+
ПРН49		+						+	+
ПРН50		+		+					+
ПРН51				+					+
ПРН52				+				+	+
ПРН53					+				+
ПРН54									
ПРН55									+
ПРН56							+		+

	ВК1.1	ВК1.2	ВК1.3	ВК1.4	ВК2.1	ВК2.2	ВК2.3	ВК2.4	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
ПРН1																						
ПРН2	+	+	+	+																		
ПРН3	+	+	+	+		+	+	+														+
ПРН4	+			+		+			+													+
ПРН5	+	+	+	+												+						+
ПРН6	+	+	+					+	+													+
ПРН7	+			+			+	+		+					+	+			+			
ПРН8							+			+					+				+			
ПРН9							+			+					+				+			
ПРН10					+				+				+									
ПРН11					+							+										
ПРН12																						
ПРН13															+							
ПРН14					+				+								+					
ПРН15					+													+			+	
ПРН16					+																	
ПРН17									+								+					
ПРН18									+									+			+	
ПРН19																						
ПРН20									+								+					
ПРН21																	+					
ПРН22										+		+							+			+
ПРН23												+										
ПРН24												+										
ПРН25												+										
ПРН26										+		+										
ПРН27									+						+							
ПРН28										+									+			
ПРН29																						
ПРН30																						

	ВК1.1	ВК1.2	ВК1.3	ВК1.4	ВК2.1	ВК2.2	ВК2.3	ВК2.4	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
ПРН31																						
ПРН32																						
ПРН33	+																					
ПРН34																						
ПРН35																						
ПРН36														+			+					
ПРН37														+			+					
ПРН38																	+					
ПРН39										+						+			+			+
ПРН40																	+					
ПРН41										+									+			+
ПРН42																						+
ПРН43							+															
ПРН44	+																					
ПРН45																						
ПРН46																						
ПРН47																						
ПРН48																						
ПРН49																	+			+		
ПРН50																	+					
ПРН51																	+				+	
ПРН52																				+		
ПРН53																		+				
ПРН54	+			+				+														
ПРН55						+					+			+								
ПРН56											+											

	ВК7. 1	ВК7. 2	ВК7. 3	ВК7. 4	ВК7. 5	ВК7. 6
ПРН1						
ПРН2						
ПРН3						
ПРН4						
ПРН5						
ПРН6						
ПРН7		+				
ПРН8		+				
ПРН9		+				
ПРН10						
ПРН11			+			+
ПРН12						
ПРН13						
ПРН14	+				+	
ПРН15					+	
ПРН16						
ПРН17						
ПРН18					+	
ПРН19						
ПРН20	+					
ПРН21						
ПРН22			+			+
ПРН23			+			+
ПРН24			+			+
ПРН25		+				+
ПРН26						+
ПРН27						

	ВК7. 1	ВК7. 2	ВК7. 3	ВК7. 4	ВК7. 5	ВК7. 6
ПРН28						
ПРН29						
ПРН30						
ПРН31						
ПРН32						
ПРН33						
ПРН34						
ПРН35						
ПРН36						
ПРН37						
ПРН38						
ПРН39						
ПРН40						
ПРН41				+		
ПРН42		+				
ПРН43				+		
ПРН44						
ПРН45						
ПРН46						
ПРН47						
ПРН48						
ПРН49						
ПРН50						
ПРН51						
ПРН52						
ПРН53	+					
ПРН54						
ПРН55						
ПРН56						

НАВЧАЛЬНИЙ ПЛАН
підготовки фахівців 2021 року вступу

Факультет інформаційних технологій

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 - Інформаційні технології
Спеціальність	125 – Кібербезпека
Освітньо-професійна програма	Кібербезпека
Орієнтація освітньої програми	освітньо-професійна програма
Форма навчання	денна
Термін навчання (обсяг кредитів ЄКТС)	3 роки 10 місяців (240)
На основі	повної загальної середньої освіти
Освітній ступінь	«Бакалавр»
Кваліфікація	Бакалавр з кібербезпеки 3439 - Фахівець із організації інформаційної безпеки

І. ГРАФІК ОСВІТНЬОГО ПРОЦЕСУ
підготовки фахівців першого (бакалаврського) рівня вищої освіти 2021 року вступу спеціальності «Кібербезпека», освітньо-професійної програми «Кібербезпека»

Рік навчання	**2021 рік**																	**2022 рік**																																		
	Вересень				27	Жовтень				Листопад				29	Грудень			27	Січень				31	Лютий			28	Березень			28	Квітень				Травень				30	Червень			27	Липень				Серпень			
	1 4	6 11	13 18	20 25	IX 2 X	4 9	11 16	18 23	25 30	1 6	8 13	15 20	22 27	XI 4 XII	6 11	13 18	20 25	XII 1 I	3 8	10 15	17 22	24 29	I 5 II	7 12	14 19	21 26	II 5 III	7 12	14 19	21 26	III 2 IV	4 9	11 16	18 23	25 30	2 7	9 14	16 21	23 28	V 4 VI	6 11	13 18	20 25	VI 2 VII	4 9	11 16	18 23	25 30	1 6	8 13	15 20	22 27
	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
I																:	:	:	-	-	-	-																:	:	:	O	O	O	O	O	O						
II																:	:	:	-	-	-	-																:	:	:	O	O	O	O	O	O						
III																:	:	:	-	-	-	-																:	:	:	X	X	X	X	X	X						
IV																:	:	:	-	-	-	-													II	II	II	II	II	//												

Умовні позначення:

	-	теоретичне навчання
:	-	екзаменаційна сесія
-	-	Канікули
X	-	виробнича практика
O	-	навчальна практика
II	-	підготовка кваліфікаційної бакалаврської роботи
//		атестація здобувачів вищої освіти (захист кваліфікаційної бакалаврської роботи)

ІІ. ПЛАН ОСВІТНЬОГО 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							
							Всього	у тому числі						I курс		II курс		III курс		IV курс	
								лекції	лабораторні	практичні				Семестри							
		Годин	(1ЄСТС 30 год).	Екзамен	Залік	Курсова робота						Навч.практика	Виробн.	1	2	3	4	5	6	7	8
														Кількість тижнів у семестрі							
														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																					
ОК1.1	Вища математика – частина1	210	7		1		90	30		60	120			6							
ОК1.2	Вища математика - частина 2	120	4	2			60	30		30	60				4						
ОК2	Фізичні основи комп'ютерної електроніки	180	6	1			120	60	60		60			8							
ОК3.1	Програмування - частина 1	180	6		1		60	30	30		120			4							
ОК3.2	Програмування - частина 2	120	4	2			75	30	45		45				5						
ОК4	Ризики інформаційної безпеки	120	4	4			60	30		30	60						4				
ОК5.1	Інформаційна безпека держави	120	4		2		75	30	45		45				5						
ОК6	Теорія інформації та кодування	120	4	2			60	30	30		60				4						
ОК7	Теорія ймовірностей, імовірнісні процеси і математична статистика	120	4	3			45	15		30	75					3					
Всього		**1290**	**43**	**6**	**3**		**645**	**285**	**210**	**150**	**645**			**18**	**18**	**3**	**4**				

1.2 Обов'язкові компоненти ОПП за рекомендацією вченої ради університету																					
ОКУ1	Правова культура особистості	120	4	3			30	15		15	90					2					
ОКУ2	Діловий протокол та етика спілкування	150	5	1			60	30		30	90			4							
ОКУ3.1	Іноземна мова - частина 1	60	2		1		30			30	30			2							
ОКУ3.2	Іноземна мова - частина 2	60	2	2			30			30	30				2						
ОКУ3.3	Іноземна мова - частина 3	60	2		3		30			30	30					2					
ОКУ3.4	Іноземна мова - частина 4	60	2	4			30			30	30						2				
ОКУ4	Філософія	120	4	5			60	30		30	60							4			
ОКУ5	Економіка та бізнес	120	4	7			30	15		15	90									2	
ОКУ6.1	Інформаційні технології - частина 1	120	4		1		60	30	30		60			4							
ОКУ6.2	Інформаційні технології - частина 2	120	4	2			60	30	30		60				4						
ОКУ7.1	Фізичне виховання - частина 1(за рахунок вільного часу студента)	30	1		1		30			30				2							
ОКУ7.2	Фізичне виховання - частина 2 (за рахунок вільного часу студента)	30	1		2		30			30					2						
ОКУ7.3	Фізичне виховання - частина 3 (за рахунок вільного часу студента)	30	1		3		30			30						2					
ОКУ7.4	Фізичне виховання - частина 4 (за рахунок вільного часу студента)	30	1		4		30			30							2				
Всього		**990**	**33**	**7**	**7**		**420**	**150**	**60**	**210**	**570**			**12**	**8**	**6**	**4**	**4**		**2**	
1.3 Вибіркові компоненти ОПП																					
Вибіркова 1 дисципліна за спеціальністю (5 семестр)																					
ВК1.1	Менеджмент	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			
ВК1.4	Безпека життєдіяльності та основи охорони праці	150	5		5		60	30		30	90							4			
Всього		**150**	**5**		**1**		**60**	**30**		**30**	**90**							**4**			

Вибіркова 1 дисципліна за спеціальністю за (6 семестр)																					
ВК2.1	Основи інтернету речей	150	5		5		60	30		30	90								4		
ВК2.2	Дискретна математика	150	5		5		60	30		30	90								4		
ВК2.3	Стандарти інформаційної та кібернетичної безпеки	150	5		5		60	30		30	90								4		
ВК2.4	Основи прогнозування та моделювання у соціальній сфері	150	5		5		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	120	4		7		30		15	15	90									2	
ВКУ2	Вибіркова дисципліна 2	120	4		7		30		15	15	90									2	
Всього		**240**	**8**		**2**		**60**		**30**	**30**	**180**									**4**	
2. ЦИКЛ СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ																					
2.1 Обов'язкові компоненти ОПП																					
ОК8.1	Комп'ютерна логіка - частина 1	90	3		2		60	30	30		30				4						
ОК8.2	Комп'ютерна логіка - частина 2	150	5	3		3,КП	75	30	45		75					5					
ОК9	Методи та засоби захисту інформації	150	5	3			90	45	45		60					6					
ОК10	Комплексні системи захисту інформації	120	4	4			60	30	30		60						4				
ОК11	Організаційне забезпечення захисту інформації	150	5	3			60	30	30		90					4					
ОК12.1	Компонентна база та схемотехніка в системах захисту інформації - частина 1	150	5		3		60	30	30		90					4					
ОК12.2	Компонентна база та схемотехніка в системах захисту інформації - частина 2	120	4	4		4,КП	60	30	30		60						4				
ОК13.1	Комп'ютерні системи - частина 1	90	3		4		60	30	30		30						4				
ОК13.2	Комп'ютерні системи - частина 2	120	4	5			45	15	30		75							3			

ОК14	Безпека інформації в інформаційно-комунікаційних системах	120	4	6			60	30	30		60								4		
ОК15	Основи криптографічного та стеганографічного захисту інформації	120	4	5			60	30	30		60							4			
ОК16.1	Системне програмування - частина 1	120	4		5		45	15	30		75							3			
ОК16.2	Системне програмування - частина 2	90	3	6		6,КП	60	30	30		30								4		
ОК17.1	Комп'ютерні мережі - частина 1	90	3		6		60	30	30		30								4		
ОК17.2	Комп'ютерні мережі - частина 2	180	6	7		7,КП	90	45	45		90									6	
ОК18	Безпека безпровідних, мобільних та хмарних технологій	120	4	4			60	30	30		60						4				
ОК19	Захист інформації в комп'ютерних системах	150	5	8			96	48	48		54										8
ОК20	Основи криптоаналізу	150	5	6			90	45	45		60								6		
ОК21	Основи технічного захисту інформації	120	4	4			60	30	30		60						4				
ОК22	Технології безпечного програмування	120	4	5		5,КП	60	30	30		60							4			
ОК23	Навчальна практика з програмування та інформаційних технологій	150	5		2							150									
ОК24	Навчальна практика з проектування систем кібербезпеки	150	5		4							150									
ОК25	Виробнича практика	150	5		6							150									
ОК26	Підготовка і захист кваліфікаційної бакалаврської роботи	150	5									**150**									
Всього		**3120**	**104**	**15**	**8**	**5**	**1311**	**633**	**678**		**1209**	**600**			**4**	**19**	**20**	**14**	**18**	**6**	**8**
Загальний обсяг обов'язкових компонентів		**5400**	**180**	**28**	**18**	**5**	**2376**	**1068**	**948**	**360**	**2424**	**600**		**30**	**30**	**28**	**28**	**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	Безпека та аудит безпроводових та рухомих мереж	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	Системний аналіз	150	5	6			60	30	30		90								4		
ВК4.3	Комп'ютерна електроніка																				
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	Ліцензування і сертифікація засобів захисту інформації	120	4	7			60	30	30		60									4	
ВК5.2	Безпека при експлуатації і обслуговуванні IT систем	120	4	7			60	30	30		60									4	
ВК5.3	Системне програмне забезпечення	120	4	7			60	30	30		60									4	
ВК5.4	Основи аудиту інформаційної безпеки	120	4	7			60	30	30		60									4	
Всього		**240**	**8**	**2**			**120**	**60**	**60**		**120**									**8**	
Вибіркова 1 дисципліна за спеціальністю за уподобанням студента (7 семестр)																					
ВК6.1	Системи моніторингу загроз та атак	120	4	7			60	30	30		60									4	
ВК6.2	Крос-платформне програмування	120	4	7			60	30	30		60									4	
ВК6.3	Інформаційно-психологічне протиборство	120	4	7			60	30	30		60									4	
Всього		**120**	**4**	**1**			**60**	**30**	**30**		**60**									**4**	

Вибіркові 4 дисципліни за спеціальністю за уподобанням студента (8 семестр)																					
ВК7.1	Безпека розробки і підтримки додатків	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
Всього		**600**	**20**	**4**			**192**	**96**	**96**		**408**										**16**
Загальний обсяг вибіркових компонентів		**1800**	**60**	**12**	**3**		**672**	**336**	**246**	**90**	**1128**							**8**	**8**	**16**	**16**
Кількість екзаменів					**40**									2	5	5	6	5	5	7	5
Кількість заліків					**21**									5	4	3	3	2	2		
Кількість курсових проектів і робіт					**5**										1	1	1	1	1	1	
Всього годин навчальних занять (без військової підготовки)		**7200**	**240**	**40**	**21**	**5**	**3048**	**1404**	**1194**	**450**	**3552**	**600**		**30**	**30**	**28**	**28**	**26**	**26**	**24**	**24**

III. СТРУКТУРА НАВЧАЛЬНОГО ПЛАНУ

Навчальні дисципліни	Години	Кредити	%
1. Обов'язкові компоненти ОПП	**5400**	**180**	**75**
2. Вибіркові компоненти ОПП	**1800**	**60**	**25**
Вибіркові дисципліни за спеціальністю	**1560**	**52**	**21,7**
Вибіркові дисципліни за уподобанням студента	**240**	**8**	**3,3**
3. Інші види навчання			

IV. ЗВЕДЕНІ ДАНІ ПРО БЮДЖЕТ ЧАСУ, ТИЖНІ

Рік навчання	Теоретичне навчання	Екзаменаційна сесія	Практична підготовка	Підготовка кваліфікаційної бакалаврської роботи	Атестація здобувачів	Канікули	Всього
1.	30	6	6			10	52
2.	30	6	6			10	52
3.	30	6	6			10	52
4.	27	6	0	5	1	4	43
Разом за ОПП	117	24	18	5	1	34	199

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	6

VI. КУРСОВІ РОБОТИ І ПРОЕКТИ

№	Назва дисципліни	Години	Кредити	Курсова робота	Курсовий проект	Семестр
1.	Комп'ютерна логіка	30	1		+	3
2.	Компонентна база та схемотехніка в системах захисту інформації	30	1		+	4
3.	Технології безпечного програмування	30	1		+	5
4.	Системне програмування	30	1		+	6
5.	Комп'ютерні мережі	30	1		+	7

VII. АТЕСТАЦІЯ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

№	Складова атестації	Години	Кредити	Кількість тижнів
1.	Підготовка і захист кваліфікаційної (бакалаврської) роботи	150	5	6