МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ЗАТВЕРДЖЕНО

Протокол № _____
від "_____"_____2019 р.

засідання вченої ради НУБіП України

Ректор_____ С. Ніколаєнко

Освітня програма вводиться в дію

з _____2019 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Кібербезпека»

першого (бакалаврського)рівня вищої освіти

за спеціальністю 125 «Кібербезпека»

галузі знань 12 «Інформаційні технології»

Кваліфікація: 3439 - Фахівець з організації інформаційної безпеки

Київ – 2019

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми
«Кібербезпека»

Проректор з навчальної

і виховної роботи_____С.М. Кваша

Начальник навчального відділу _____О.В. Зазимко

Декан факультету _____О.Г. Глазунова

Керівник проектної групи _____В.А. Лахно

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.
2. **Шкарупило Вадим Вікторович, кандидат технічних наук, доцент кафедри комп'ютерних систем і мереж**.
3. **Іваник Юлія Юріївна**, кандидат технічних наук, доцент кафедри комп'ютерних систем і мереж.
4. **Блозва Андрій Петрович,** кандидат педагогічних наук, доцент кафедри комп'ютерних систем і мереж

Освітньо-професійна програма «**Кібербезпека**» підготовки фахівців першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «**Кібербезпека**» розроблена відповідно до Закону України «Про вищу освіту» від 01.07.2014 р., Постанов Кабінету Міністрів України від 23.11.2011 р. «Про затвердження Національної рамки кваліфікацій» від 30.12.2015 р. № 1187, «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30.12.2015 р., методичних рекомендацій «Розроблення освітніх програм. Методичні рекомендації» (2014 р.).

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. Фахівець із організації інформаційної безпеки
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний 240 кредитів ЄКТС, термін навчання 4 роки
Наявність акредитації	Ліцензується вперше.
Цикл/рівень	Перший (бакалаврський) рівень FQ-EHEA – перший цикл, EQF LLL – 6 рівень, НРК – 7 рівень / Бакалавр
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 1 липня 2023 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 і спроможності з автономною діяльністю та відповідальністю під час вирішення завдань та проблемних питань в галузі інформаційної безпеки; забезпечення якісної теоретичної та практичної підготовки у вигляді знань, умінь та навичок за спеціальністю 125 «Кібербезпека» для організації та забезпечення інформаційної безпеки на об'єктах інформаційної діяльності.	
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 ІТ 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 інш.; 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	Бакалавр зі спеціальності «Кібербезпека» має право продовжити навчання для отримання ОС «Магістр» за

	спеціальності «Кібербезпека» або інших споріднених спеціальностей. Концепція освітньої програми підготовки фахівців відповідає освітнім програмам підготовки бакалаврів закордонних університетів «Bachelor of Science in Computer Engineering». Освітня програма надає можливість продовжувати навчання бакалаврів за кордоном і забезпечує академічну мобільність в межах України.
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" (2015 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 (ЗК)	**КЗ1**. Здатність застосовувати знання у практичних ситуаціях. **КЗ2**. Знання та розуміння предметної області та розуміння професії. **КЗ3**. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. **КЗ4**. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. **КЗ5**. Здатність до пошуку, оброблення та аналізу інформації. **КЗ6**. 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; **КЗ7**. 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. **КЗ8**. Здатність до абстрактного і системного мислення, аналізу та синтезу.
Фахові компетентності спеціальності (ФК)	**ФК1**. 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. **ФК2**. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. **ФК3**. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. **ФК4**. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. **ФК5**. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. **ФК6**. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. **ФК7**. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

	ФК8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. **ФК9**. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. **ФК10**. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. **ФК11**. Здатність виконувати моніторинг процесів функціонування Інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. **ФК12**. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки. **ФК13**. 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 та методи 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 – 62 в т.ч. - академіки, члени-кореспонденти НАН України та НААН України – 1 - академіки громадських академій – 2 - доктори наук, професори – 12 - кандидати наук, доценти – 26 - кандидати наук, асистенти – 4 - асистенти без наукового ступеня – 22
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 комп'ютерів, що експлуатуються, становить 6 років. У навчальному процесі функціонують лабораторії: проектування цифрових пристроїв (розгорнуто навчально-лабораторні 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 лайками Майкрософт), Веб-технологій (розробка веб-орієнтованих систем), інформаційних управляючих систем (програмне забезпечення для проектування та розробки інформаційних систем), комп'ютерного моніторингу довкілля (апаратно-програмні засоби на платформі Arduino: мікроконтролери, датчики, мікросхеми та плати для виготовлення спеціалізованих комп'ютерів), лекційні аудиторії обладнані мультимедійними проекторами, екранами, IP-камерами для системи відео спостереження. В підрозділах факультету функціонує 236 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 – загальноуніверситетського 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. Бібліотечний фонд багатогалузевий, нараховує понад один мільйон примірників вітчизняної та зарубіжної літератури, у т.ч. рідкісних видань, спец. видів науково-технічної літератури і документів (з 1984 р.), авторефератів дисертацій (з 1950 р.), дисертацій (з 1946 р.), більше 500 назв 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 професорсько-викладацького складу, аспірантів та

	магістрів – Reference Room; МБА; каталоги, в т.ч. електронний (понад 180000 одиниць записів); бібліографічні картотеки в тому числі персоналії (з 1954 р.); фонд довідкових і бібліографічних видань Така розгалужена система бібліотеки дає можливість щорічно обслуговувати всіма структурними підрозділами понад 40000 користувачів у рік, у т.ч. 14000 студентів. Книговидача становить більше мільйона примірників у рік. Читальний зал забезпечений бездротовим доступом до мережі Інтернет. Всі ресурси бібліотеки доступні через сайт університету: https://library.nubip.edu.ua. З 1 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. 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	В 2017 році укладено 3 нові угоди про співробітництво у рамках Програми «Еразмус+»: «Кредитна мобільність» за результатами конкурсу 2016-2021 років університет уклав Міжінституційні угоди на реалізацію академічної мобільності із 20 європейськими університетами: Латвійський сільськогосподарський університет; Університетом екології та менеджменту в Варшаві, Польща; Варшавський університет наук про життя, Польща; Університетом Александраса Стульгінскіса, Литва; Університет Агрісуп, Діжон, Франція; Університетом Фоджа, Італія; Університет Дікле, Туреччина; Технічний університет Зволен, Словаччина; Вроцлавський університет наук про життя, Польща; Вища школа сільського господарства м Лілль, Франція; Університет короля Міхаіла 1, Тімішоара, Румунія; Університет прикладних наук Хохенхайм, Німеччина; Норвезький університет наук про життя. Норвегія; Шведський університет сільськогосподарських наук, UPSALA; Університет Ллейда, Іспанія; Університет прикладних наук

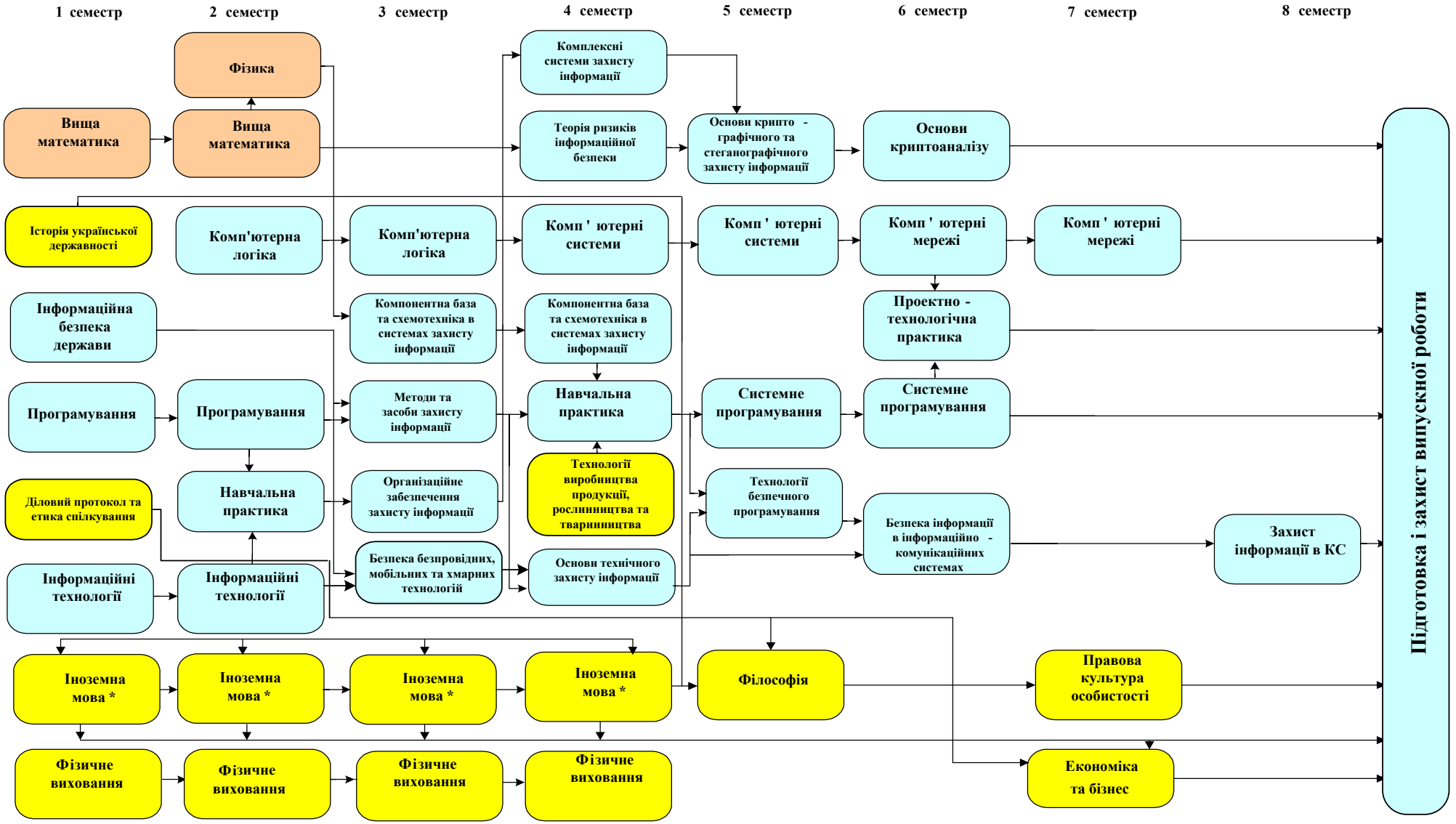
	Вайєнштефан-Тріздорф, Німеччина; Загребський університет, Хорватія; Неапольський Університет Федеріка 2, Італія; Університетом м. Тарту, Естонія; Словацьким аграрним університетом, м. Нітра. 1.Угода про співробітництво та організацію взаємовідносин з Університетом аграрних наук м. Клуж Напока (Румунія) - №75 від 29.06.2017 р. 2. Угода про співробітництво та організацію взаємовідносин з Інститутом зоології Словацької Академії Наук - №38 від 11.04.2017 р. 3. Угода про співробітництво та організацію взаємовідносин з Університетом ветеринарної медицини та фармації в Кошице Словацької республіки (2013 р.) 4. Угода про співробітництво та організацію взаємовідносин з Вроцлавським природничим університетом (Польща) - №334 від 6.11.2013 р. 5. Угода про співробітництво та організацію взаємовідносин з Самарською ДСГА – від 25.09.2013 р. У 2017 році запроваджено програму подвійних дипломів з Поморською академію в м. Слупськ (Польща) для студентів факультету інформаційних технологій. Запроваджено співпрацю щодо обміну студентами спеціальності комп'ютерних наук з Технічним Університетом Юлдіз (м. Стамбул, Туреччина) та Університетом Акдениз (м. Анталія, Туреччина). У відповідності до програми Mevlana четверо студентів 4 курсу ОС "Бакалавр" відібрані на навчання в Університет Акдениз (м. Анталія, Туреччина) у 2018-2019 навчальному році: Анна Гавриленко, Олександр Волохов, Дар'я Хомич та Богдан Настенко. У 2017-2018 н.р. студенти факультету у відповідності до програми Erasmus+ навчалися у Варшавському університеті наук про життя, Польща (Глазунов А.); в Університеті Фоджа, Італія (Плиска Л.). У 2018-2019 навчальному році двоє студентів 1 року навчання ОС "Магістр" Юрій Нам'ясенко та Максим Колісник подали документи на навчання в Варшавський університет наук про життя, м. Варшава, Польща.
Навчання іноземних здобувачів вищої освіти	Навчання іноземних здобувачів вищої освіти може проводитися на загальних умовах з додатковою мовною підготовкою. На факультеті інформаційних технологій на навчання залучено 7 іноземних студентів на спеціальність "Комп'ютерні науки".

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

2.1. Перелік обов'язкових 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			
1.1 Обов'язкові компоненти ОПП			
ОК1.	Вища математика	12	екзамен
ОК2.	Фізика	6	екзамен
ОК3.	Програмування	11	екзамен
ОК4.	Теорія ризиків інформаційної безпеки	4	екзамен
ОК5.	Інформаційна безпека держави	4	екзамен
1.2 Обов'язкові компоненти ОПП за рішенням вченої ради університету			
ОК6.	Правова культура особистості	3	екзамен
ОК7.	Діловий протокол та етика спілкування	4	екзамен
ОК8	Технології виробництва продукції рослинництва та тваринництва	4	екзамен
ОК9	Історія української державності	4	екзамен
ОК10	Іноземна мова	6	екзамен
ОК11	Філософія	4	екзамен
ОК12	Економіка та бізнес	4	екзамен
ОК13	Інформаційні технології	6	екзамен
ОК14	Фізичне виховання	4	залік
2. ЦИКЛ СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
2.1 Обов'язкові компоненти ОПП			
ОК15.	Комп'ютерна логіка	10	екзамен
ОК16.	Методи та засоби захисту інформації	5	екзамен
ОК17.	Комплексні системи захисту інформації	4	екзамен
ОК18.	Організаційне забезпечення захисту інформації	6	екзамен
ОК19.	Компонентна база та схемотехніка в системах захисту інформації	10	екзамен
ОК20.	Комп'ютерні системи	7	екзамен
ОК21.	Безпека інформації в інформаційно-комунікаційних системах	4	екзамен
ОК22.	Основи криптографічного та стеганографічного захисту інформації	4	екзамен
ОК23.	Системне програмування	7	екзамен
ОК24.	Комп'ютерні мережі	6	екзамен
ОК25.	Безпека безпровідних, мобільних та хмарних технологій	5	екзамен
ОК26.	Захист інформації в комп'ютерних системах	5	екзамен
ОК27.	Основи криптоаналізу	5	екзамен
ОК28.	Основи технічного захисту інформації	4	екзамен
ОК29.	Технології безпечного програмування	4	екзамен
ОК30.	Навчальна практика з програмування	6	екзамен
ОК31.	Навчальна практика з технологій захисту інформації	6	екзамен
ОК32.	Проектно-технологічна практика	5	залік
ОК33.	Дипломне проектування і захист кваліфікаційної роботи	5	Захист роботи
Загальний обсяг обов'язкових компонентів		**180**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

2.2. Структурно-логічна схема підготовки фахівців



* - Використовується у багатьох дисциплінах

3. Форми атестації здобувачів вищої освіти

Атестація здобувачів першого (бакалаврського) освітньо-професійного рівня за спеціальністю «Кібербезпека» здійснюється у формі захисту дипломного проекту та завершується видачею документа встановленого зразка про присудження йому ступеня бакалавра з присвоєнням кваліфікації «Фахівець з організації інформаційної безпеки»:

Атестація здобувачів вищої освіти проводиться екзаменаційною комісією відповідно до вимог ОПП. До складу екзаменаційної комісії можуть включатися представники роботодавців та їх об'єднань, відповідно до положення про екзаменаційну комісію, затвердженого вченою радою закладу освіти.

До атестації допускаються студенти, які виконали всі вимоги програми підготовки (навчального плану). На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою в процесі навчання. Термін проведення атестації визначається навчальним планом та графіком освітнього процесу.

Атестація здійснюється відкрито у формі публічного захисту бакалаврської роботи.

Кваліфікаційний проект/робота має передбачати розв'язання спеціалізованої задачі в галузі інформаційної та/або кібербезпеки. Кваліфікаційний проект/ робота має бути перевірений на плагіат.

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

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22
КЗ1		+	+	+	+	+	+	+		+		+	+							+	+	+
КЗ2				+	+								+				+				+	+
КЗ3			+				+			+								+			+	
КЗ4				+	+																+	+
КЗ5										+								+				
КЗ6						+	+		+		+					+						
КЗ7					+	+	+		+		+	+		+								
КЗ8	+	+	+	+							+				+				+	+		+
ФК1					+	+							+									
ФК2																					+	
ФК3																				+	+	
ФК4												+										
ФК5				+												+					+	
ФК6																+						
ФК7																	+	+		+	+	
ФК8																+	+	+				
ФК9																+	+	+	+			
ФК10																+	+					+
ФК11																	+					
ФК12																+	+					
ФК13															+				+			

	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33
К31	+	+	+	+	+	+	+	+	+	+	+
К32		+	+	+	+	+	+	+	+	+	+
К33									+	+	+
К34		+	+	+	+	+		+	+		+
К35							+		+		+
К36											
К37											
К38				+	+		+		+		+
ФК1			+				+		+		+
ФК2		+	+	+			+		+		+
ФК3	+	+	+	+		+	+		+	+	+
ФК4											+
ФК5		+	+	+		+			+		+
ФК6		+	+	+					+	+	+
ФК7		+	+			+			+		+
ФК8											+
ФК9			+						+		+
ФК10				+	+	+					+
ФК11		+	+			+			+		+
ФК12			+	+					+		+
ФК13	+			+			+		+		+

5. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньої програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22
ПРН1							+			+												
ПРН2								+				+										
ПРН3			+										+		+				+		+	+
ПРН4															+				+		+	+
ПРН5													+			+		+				
ПРН6				+					+		+					+		+			+	
ПРН7					+	+												+				
ПРН8					+													+				
ПРН9					+													+				
ПРН10															+		+			+		
ПРН11																	+					
ПРН12																+						
ПРН13				+												+	+				+	
ПРН14																					+	
ПРН15			+										+									
ПРН16																	+					
ПРН17																				+	+	
ПРН18																			+			
ПРН19				+												+						+
ПРН20																	+				+	
ПРН21																+	+				+	
ПРН22																+	+					
ПРН23																+	+				+	
ПРН24																+	+					

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22
ПРН25																+	+	+				
ПРН26																+		+				
ПРН27				+												+						
ПРН28																+	+	+				
ПРН29				+																	+	
ПРН30				+																	+	
ПРН31				+												+					+	
ПРН32				+														+				
ПРН33				+																		
ПРН34																		+				
ПРН35																	+					
ПРН36																+	+					
ПРН37															+	+	+		+	+		
ПРН38															+	+	+		+	+		
ПРН39																		+				
ПРН40																		+	+			
ПРН41																		+				
ПРН42																		+				
ПРН43				+	+																	
ПРН44				+																		
ПРН45				+													+					
ПРН46				+																		
ПРН47																						+
ПРН48																						+
ПРН49																+						

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22
ПРН50																+	+				+	
ПРН51																					+	
ПРН52																					+	
ПРН53																						
ПРН54						+	+		+													
ПРН55	+	+																				
ПРН56															+				+	+		

	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33
ПРН1									+		+
ПРН2											+
ПРН3								+	+	+	+
ПРН4										+	+
ПРН5						+			+		+
ПРН6				+					+		+
ПРН7									+		+
ПРН8									+		+
ПРН9											+
ПРН10											+
ПРН11		+	+								+
ПРН12				+					+		+
ПРН13		+	+			+					+
ПРН14	+	+	+	+		+	+				+
ПРН15	+						+				+
ПРН16											+
ПРН17		+	+			+					+
ПРН18						+					+
ПРН19				+	+						+
ПРН20										+	+
ПРН21							+		+	+	+
ПРН22						+			+	+	+

	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33
ПРН23				+		+			+		+
ПРН24	+			+		+			+		+
ПРН25			+						+		+
ПРН26									+		+
ПРН27		+	+								+
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									+		+

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Розглянуто і схвалено
Вченою радою НУБІП України
"_____" _____ 2019 р.
(Протокол № ____)

"ЗАТВЕРДЖУЮ"
Ректор НУБІП України
_____ С.НІКОЛАЄНКО
"_____" _____ 2019 р.

НАВЧАЛЬНИЙ ПЛАН

підготовки фахівців 2019 року вступу

Рівень вищої освіти (ОКР)	перший (бакалаврський)
Галузь знань	12 - Інформатика та обчислювальна техніка
Спеціальність	125 - Кібербезпека
Форма навчання	денна
Термін навчання (обсяг кредитів ЄКТС)	4 роки (240 кредитів)
На основі	повної загальної середньої освіти
Ступінь вищої освіти	"Бакалавр"
Кваліфікація	Фахівець з організації інформаційної безпеки

І. ГРАФІК НАВЧАЛЬНОГО ПРОЦЕСУ
підготовки фахівців ОКР "Бакалавр" 2019 року вступу
напряму підготовки "Кібербезпека"

Курс	2019																		2020							
	Вересень					Жовтень				Листопад				Грудень					Січень				Лютий			
	1	7	14	21	28	5	12	19	26	2	9	16	23	30	7	14	2	28	4	11	18	25	1	8	15	22
	5	12	19	26	4	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30	6	13	20	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
I																:	:	-	-	-	-	-				
II																:	:	-	-	-	-	-				
III																:	:	-	-	-	-	-				
IV																:	:	-	-	-	-	-				

Курс	2020																									
	Березень					Квітень				Травень				Червень					Липень				Серпень			
	29	7	14	21	28	4	11	18	25	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22
	5	12	19	26	2	9	16	23	30	7	14	21	28	4	11	18	25	2	9	16	23	30	6	13	20	27
	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												:	:	:	о	о	о	о	о	о	-	-	-	-	-	-
II												:	:	:	о	о	о	о	о	о	-	-	-	-	-	-
III												:	:	:	х	х	х	х	х	х	-	-	-	-	-	-
IV									:	:	:	//	//	//	//	//	II	II								

Умовні позначення:

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

№ 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		Навчальна практика	Виробна практика	Семестри							
		Годин	(1ЄСТС 30 год). кредитів	Екзамен	Залік	Курсова робота (проект)								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 - частина 1	240	8		1		90	30		60	150			6							
ОК1.2	Вища математика - частина 2	120	4	2			60	30		30	60				4						
ОК2	Фізика	180	6	2			120	60	60		60				8						
ОК3.1	Програмування - частина 1	180	6		1		90	30	60		90			6							
ОК3.2	Програмування - частина 2	150	5	2		2,КР	75	30	45		75				5						
ОК4	Теорія ризиків інформаційної безпеки	120	4	4			60	30		30	60						4				
ОК5	Інформаційна безпека держави	120	4	1			60	30	30		60			4							
Всього		1110	37	5	2	1	555	240	195	120	555			16	17		4				
1.2 Обов'язкові компоненти ОПП за рішенням вченої ради університету																					
ОК6	Правова культура особистості	90	3	7			30	15		15	60									2	
ОК7	Діловий протокол та етика спілкування	120	4	1			60	30		30	60			4							
ОК8	Технології виробництва продукції рослинництва та тваринництва	120	4	4			60	30		30	60						4				
ОК9	Історія української державності	120	4	1			30	15		15	90			2							
ОК10.1	Іноземна мова - частина 1	30	1		1		30			30				2							
ОК10.2	Іноземна мова - частина 2	60	2	2			30			30	30				2						
ОК10.3	Іноземна мова - частина 3	60	2		3		30			30	30					2					
ОК10.4	Іноземна мова - частина 4	30	1	4			30			30							2				
ОК11	Філософія	120	4	5			60	30		30	60							4			
ОК12	Економіка та бізнес	120	4	7			30	15		15	90									2	
ОК13.1	Інформаційні технології - частина 1	90	3		1		60	30	30		30			4							
ОК13.2	Інформаційні технології - частина 2	90	3	2			60	30	30		30				4						
ОК14.1	Фізичне виховання - частина 1	30	1		1		30			30				2							
ОК14.2	Фізичне виховання - частина 2	30	1		2		30			30					2						
ОК14.3	Фізичне виховання - частина 3	30	1		3		30			30						2					
ОК14.4	Фізичне виховання - частина 4	30	1		4		30			30							2				
Всього		1050	35	9	7		510	195	60	255	540			14	8	4	8	4		4	
1.3 Вибіркові компоненти ОПП																					
Вибіркова 1 дисципліна за уподобанням студента (5 семестр)																					
ВК1.1.1	Менеджмент	150	5		5		30	15		15	120							2			
ВК1.1.2	Техніка і технології в АПК																				
ВК1.1.3	Типові технологічні об'єкти с.-г. виробництва																				
ВК1.1.4	Безпека життєдіяльності та основи охорони праці																				
Всього		150	5		1		30	15		15	120							2			
Вибіркова 1 дисципліна за уподобанням студента (6 семестр)																					
ВК1.2.1	Основи інтернету речей	150	5	6			60	30		30	90								4		
ВК1.2.2	Дискретна математика																				

ВК1.2.3	Стандарти інформаційної та кібернетичної безпеки																				
ВК1.2.4	Основи прогнозування та моделювання у соціальній сфері																				
Всього		150	5	1			60	30		30	90								4		
Вибіркові дисципліни за уподобанням студента (7 семестр)																					
ВК1.3.1	Вибіркова дисципліна 1	90	3	7			30	15	15		60									2	
ВК1.3.2	Вибіркова дисципліна 2	90	3	7			30	15	15		60									2	
Всього		180	6	2			60	30	30		120									4	
2. ЦИКЛ СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ																					
2.1 Обов'язкові компоненти ОПП																					
ОК15.1	Комп'ютерна логіка - частина 1	120	4	2			75	30	45		45				5						
ОК15.2	Комп'ютерна логіка - частина 2	180	6	3		3,КП	75	30	45		105					5					
ОК16	Методи та засоби захисту інформації	150	5	3			75	45	30		75					5					
ОК17	Комплексні системи захисту інформації	120	4	4			60	30	30		60						4				
ОК18	Організаційне забезпечення захисту інформації	180	6	3			75	30	45		105					5					
ОК19.1	Компонентна база та схемотехніка в системах захисту інформації - частина 1	180	6	3			75	30	45		105					5					
ОК19.2	Компонентна база та схемотехніка в системах захисту інформації - частина 2	120	4	4		4,КП	60	30	30		60						4				
ОК20.1	Комп'ютерні системи - частина 1	90	3		4		60	30	30		30						4				
ОК20.2	Комп'ютерні системи - частина 2	120	4	5			60	30	30		60							4			
ОК21	Безпека інформації в інформаційно-комунікаційних системах	120	4	6			60	30	30		60								4		
ОК22	Основи криптографічного та стеганографічного захисту інформації	120	4	5			60	30	30		60							4			
ОК23.1	Системне програмування - частина 1	120	4		5		60	30	30		60							4			
ОК23.2	Системне програмування - частина 2	90	3	6		6,КР	60	30	30		30								4		
ОК24.1	Комп'ютерні мережі - частина 1	90	3		6		60	30	30		30								4		
ОК24.2	Комп'ютерні мережі - частина 2	90	3	7		7,КП	60	30	30		30									4	
ОК25	Безпека безпровідних, мобільних та хмарних технологій	150	5	3			60	30	30		90					4					
ОК26	Захист інформації в комп'ютерних системах	150	5	8			96	48	48		54										8
ОК27	Основи криптоаналізу	150	5	6			90	45	45		60								6		
ОК28	Основи технічного захисту інформації	120	4	4			60	30	30		60						4				
ОК29	Технології безпечного програмування	120	4	5		5,КР	60	30	30		60							4			
Всього		2580	86	17	3	5	1341	648	693		1239				5	24	16	16	18	4	8
2.2 Обов'язкові компоненти ОПП за рішенням вченої ради університету																					
ОК30	Навчальна практика з програмування	180	6		2							180									
ОК31	Навчальна практика з технологій захисту інформації	180	6		4							180									
ОК32	Проектно-технологічна практика	150	5		6							150									
ОК33	Дипломне проектування і захист кваліфікаційної роботи	150	5									150									
Всього		660	22		3							660									
2.3 Вибіркові компоненти ОПП																					
Вибіркова 1 дисципліна за уподобанням студента (5 семестр)																					
ВК2.1.1	Прикладні аспекти побудови систем захисту інформації	150	5	5			60	30	30		90							4			
ВК2.1.2	Безпека та аудит безпроводових та рухомих мереж																				
ВК2.1.3	Паралельні та розподілені обчислення																				
Всього		150	5	1			60	30	30		90							4			
Вибіркова 1 дисципліна за уподобанням студента (6 семестр)																					
ВК2.2.1	Управління доступом	150	5	6			60	30	30		90								4		
ВК2.2.2	Системний аналіз																				

ВК2.2.3	Комп'ютерна електроніка																				
ВК2.2.4	Управління проектами розробки систем захисту інформації																				
Всього		150	5	1			60	30	30		90								4		
Вибіркові 2 дисципліни за уподобанням студента (7 семестр)																					
ВК2.3.1	Ліцензування і сертифікація засобів захисту інформації	150	5	7			60	30	30		90									4	
ВК2.3.2	Безпека при експлуатації і обслуговуванні IT систем	150	5	7			60	30	30		90									4	
ВК2.3.3	Системне програмне забезпечення																				
ВК2.3.4	Основи аудиту інформаційної безпеки																				
Всього		300	10	2			120	60	60		180									8	
Вибіркова 1 дисципліна за уподобанням студента (7 семестр)																					
ВК2.4.1	Системи моніторингу загроз та атак	120	4	7			60	30	30		60									4	
ВК2.4.2	Крос-платформне програмування																				
ВК2.4.3	Інформаційно-психологічне протиборство																				
Всього		120	4	1			60	30	30		60									4	
Вибіркові 4 дисципліни за уподобанням студента (8 семестр)																					
ВК2.5.1	Безпека розробки і підтримки додатків	150	5	8			48	24	24		102										4
ВК2.5.2	Проведення розслідувань інцидентів інформаційної безпеки	150	5	8			48	24	24		102										4
ВК2.5.3	Управління веб-контентом	150	5	8			48	24	24		102										4
ВК2.5.4	Продукти та послуги інформаційної безпеки	150	5	8			48	24	24		102										4
ВК2.5.5	Програмування в середовищі сучасних ОС																				
ВК2.5.6	Адміністрування комп'ютерних мереж																				
Всього		600	20	4			192	96	96		408										16
Всього за обов'язковими дисциплінами ОПП		5400	180	31	15	6	2406	1083	948	375	2334	660		30	30	28	28	20	18	8	8
	Військова підготовка	870	29								434										
Всього за вибірковими дисциплінами ОПП		1800	60	12	1		642	321	276	45	1158							6	8	16	16
ЗАГАЛЬНА КІЛЬКІСТЬ ГОДИН ЗА ОПП		7200	240	43	16	6	3048	1404	1224	420	3492	660		30	30	28	28	26	26	24	24
	Кількість екзаменів				43									3	6	5	6	5	5	8	5
	Кількість заліків				16									5	2	2	3	2	2		
	Кількість курсових проектів і робіт				6										1	1	1	1	1	1	

III. СТРУКТУРА НАВЧАЛЬНОГО ПЛАНУ

Навчальні дисципліни	**Години**	**Кредити**	**%**
1. Обов'язкові компоненти ОПП	5400	180	75,0
2. Вибіркові компоненти ОПП	1800	60	25,0
Вибіркові дисципліни за спеціальністю	1470	49	20,4
Вибіркові дисципліни за уподобанням студента	330	11	4,6
3. Інші види навчання			
Разом за ОПП	**7200**	**240**	**100,0**

IV. ЗВЕДЕНІ ДАНІ ПРО БЮДЖЕТ ЧАСУ, ТИЖНІ

Рік навчання	Теоретичне навчання	Екзаменаційна сесія	Практична підготовка	Підготовка бакалаврської роботи	Атестація	Канікули	Всього
1	30	5	6			11	52
2	30	5	6			11	52
3	30	5	6			11	52
4	27	5	0	5	2	5	44
Разом за ОПП	**117**	**20**	**18**	**5**	**2**	**38**	**200**

V. ПРАКТИЧНА ПІДГОТОВКА

№	Вид практики	Семестр	Години	Кредити	Кількість тижнів
1	Навчальна практика з програмування	2	180	6	6
2	Навчальна практика з технологій захисту інформації	4	180	6	6
3	Проектно-технологічна практика	6	150	5	6

VI. КУРСОВІ РОБОТИ І ПРОЕКТИ

№	Назва дисципліни	Години	Кредити	Курсова робота	Курсовий проект	Семестр
1	Програмування	15	0,5	+		2
2	Комп’ютерна логіка	30	1		+	3
3	Компонентна база та схемотехніка в системах захисту інформації	30	1		+	4
4	Технології безпечного програмування	15	0,5	+		5
5	Системне програмування	15	0,5	+		6
6	Комп’ютерні мережі	30	1		+	7

VII. АТЕСТАЦІЯ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

№	Складова атестації	Години	Кредити	Кількість тижнів
1	Захист бакалаврської роботи	60	2	2