МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ЗАТВЕРДЖЕНО

Протокол № 10 від "24" квітня 2019 р.
засідання вченої ради НУБіП України

Освітньо-професійна програма
вводиться в дію з 2 вересня 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

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 **,керівник проектної групи**
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», стандарту вищої освіти, наказу НУБІП України «Про розроблення освітніх програм підготовки бакалаврів і магістрів в університеті для вступників 2019 р.» від 21.02.2019 р. № 161.

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 IT-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 IT 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 програма 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)	**К31**. Здатність застосовувати знання у практичних ситуаціях. **К32**. Знання та розуміння предметної області та розуміння професії. **К33**. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. **К34**. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. **К35**. Здатність до пошуку, оброблення та аналізу інформації. **К36**. 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; **К37**. 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. **К38**. 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, одо 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 – 2 - доктори наук, професори – 12 - кандидати наук, доценти – 28 - 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. 3 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 11.04.2017р. 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 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	12	екзамен
ОК2.	Фізика	6	екзамен
ОК3.	Програмування	11	екзамен
ОК4.	Методи та засоби захисту інформації	5	екзамен
Вибіркові компоненти ОПП			
Вибірковий блок (за вибором університету)			
ВУ1.	Правова культура особистості	4	екзамен
ВУ2.	Діловий протокол та етика спілкування	4	екзамен
ВУ3.	Технології виробництва продукції рослинництва та тваринництва	4	екзамен
ВУ4.	Історія української державності	4	екзамен
ВУ5.	Іноземна мова	4	екзамен
ВУ6.	Філософія	4	екзамен
ВУ7.	Економіка та бізнес	4	екзамен
ВУ8.	Інформаційні технології	6	екзамен
ВУ9.	Фізичне виховання	4	залік
2. ЦИКЛ СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
Обов'язкові компоненти ОПП			
ОК5.	Комп'ютерна логіка	10	екзамен
ОК6.	Комплексні системи захисту інформації	4	екзамен
ОК7.	Інформаційна безпека держави	4	екзамен
ОК8.	Основи технічного захисту інформації	4	екзамен
ОК9.	Організаційне забезпечення захисту інформації	6	екзамен
ОК10.	Компонентна база та схемотехніка в системах захисту інформації	10	екзамен
ОК11.	Теорія ризиків інформаційної безпеки	4	екзамен
ОК12.	Безпека інформації в інформаційно-комунікаційних системах	4	екзамен
ОК13.	Архітектура та програмування мікроконтролерів	8	екзамен
ОК14.	Технології захисту інформації	4	екзамен
ОК15.	Основи криптоаналізу	4	екзамен
ОК16.	Системне програмування	7	екзамен
ОК17.	Комп'ютерні мережі	8	екзамен
ОК18.	Основи криптографічного та стеганографічного захисту інформації	4	екзамен
ОК19.	Комп'ютерні системи	3	екзамен
ОК20.	Захист інформації в комп'ютерних системах	5	екзамен

ОК21.	Системне програмне забезпечення	8	екзамен
ОК22.	Проектно-технологічна практика	6	залік
ОК23.	Підготовка і захист бакалаврської роботи	7	Захист роботи
Загальний обсяг обов'язкових компонентів		**144**	
Вибіркові компоненти ОПП			
Дисципліни за вибором університету			
ВУ1.	Правова культура особистості	4	екзамен
ВУ2.	Діловий протокол та етика спілкування	4	екзамен
ВУ3.	Технології виробництва продукції рослинництва та тваринництва	4	екзамен
ВУ4.	Історія української державності	4	екзамен
ВУ5.	Іноземна мова	4	екзамен
ВУ6.	Філософія	4	екзамен
ВУ7.	Економіка та бізнес	4	екзамен
ВУ8.	Інформаційні технології	6	екзамен
ВУ9.	Фізичне виховання	4	залік
Загальний обсяг компонентів за вибором університету		**36**	
Вибірковий блок 1 (за вибором студента)			
Вибірковий блок 1 «Безпека інформаційно-комунікаційних систем»			
ВБ1.1.	Управління доступом	4	екзамен
ВБ1.2.	Системний аналіз	4	екзамен
ВБ1.3.	Об'єктно-орієнтоване програмування	5	екзамен
ВБ1.4.	Ліцензування і сертифікація засобів захисту інформації	4	екзамен
ВБ1.5.	Захищені мережеві технології обробки інформації	5	екзамен
ВБ1.6.	Безпека при експлуатації і обслуговуванні IT систем	4	екзамен
ВБ1.7.	Крос-платформне програмування	4	екзамен
ВБ1.8.	Безпека розробки і підтримки додатків	4	екзамен
ВБ1.9.	Навчальна практика з програмування	6	залік
ВБ1.10.	Навчальна практика з проектування цифрових пристроїв	6	залік
ВБ1.11.	Адміністрування комп'ютерних мереж	5	екзамен
ВБ1.12.	Управління проектами захисту інформації	4	екзамен
ВБ1.13.	Програмування в середовищі сучасних ОС	5	екзамен
Вибірковий блок 2 (за вибором студента)			
Вибірковий блок 2 «Управління інформаційною безпекою»			
ВБ2.1.	Технології комп'ютерного проектування систем захисту інформації	4	екзамен
ВБ2.2.	Системи прийняття рішень в завданнях захисту інформації	4	екзамен
ВБ2.3.	Сучасні технології програмування	5	екзамен
ВБ2.4.	Безпека безпровідних, мобільних та хмарних технологій	4	екзамен
ВБ2.5.	Основи аудиту інформаційної безпеки	5	екзамен
ВБ2.6.	Архітектура і моделі безпеки	4	екзамен
ВБ2.7.	Програмування на мові Java	4	екзамен
ВБ2.8.	Проведення розслідувань інцидентів	4	екзамен

	інформаційної безпеки		
ВБ2.9.	Навчальна практика з комп'ютерних технологій	6	залік
ВБ2.10.	Навчальна практика з систем захисту інформації	6	залік
ВБ2.11.	Управління веб-контентом	5	екзамен
ВБ2.12.	Продукти та послуги інформаційної безпеки	4	екзамен
ВБ2.13.	Розробка додатків в сучасних ОС	5	екзамен
Загальний обсяг вибіркових компонентів:		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

2.2. Структурно-логічна схема підготовки фахівців

2.3. Обов’язкові компоненти ОПП

1. ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ
Обов’язкові компоненти ОПП

Вища математика (Частини 1 та 2). Вивчаються наступні теми: Математичний аналіз. Комплексні числа. Елементарні функції. Неперервність функцій. Похідна та диференціал функції. Дослідження функцій. Інтеграли. Функції декількох змінних. Екстремум функції. Ряди. Диференційні рівняння. Звичайні диференційні рівняння першого порядку. Задача Коші. Лінійна алгебра. Векторна алгебра. Аналітична геометрія. Системи лінійних алгебраїчних рівнянь. Лінійні простори та лінійні оператори.

Фізика. Вивчаються наступні теми: Механіка. Кінематика і динаміка. Моделі класичної механіки. Робота та енергія. Основи теорії відносності. Електрика і магнетизм. Електричне поле. Постійний електричний струм. Змінний електричний струм. Магнітне поле. Електромагнітна індукція. Рівняння Максвела. Оптика. Хвильова оптика. Інтерференція. Дифракція. Поляризація. Дисперсія. Квантова фізика. Теплове випромінювання. Фотони. Модель атома. Рівняння Шрьодингера. Елементи фізики твердого тіла.

Програмування - частина 1. В першій частині курсу «Програмування» розглядаються наступні теми: Основні поняття та проблеми розробки ПЗ. Життєвий цикл ПЗ; міжнародні стандарти життєвого циклу ПЗ. Моделі та методології розробки ПЗ. Аналіз, специфікація, верифікація та валідація вимог до ПЗ. Проектування архітектури ПЗ. Шаблони проектування ПЗ. Проектування інтерфейсу користувача. Методології моделювання SADT, IDEF, DFD, ELM, OOAD. Мови моделювання. Поведінкове моделювання. Діаграми станів, діяльності, взаємодії, послідовності, часові. Структурне моделювання. Функціональне моделювання. Моделювання потоків даних.

Програмування - частина 2. В другій частині курсу «Програмування» розглядаються наступні теми: Засоби автоматизації моделювання. Задачі управління проектами. Управління ризиками програмного проекту. Контроль та моніторинг стану проекту. Організація роботи проектної команди. Ролі та зони відповідальності учасників команди. Якість ПЗ; стандарти якості ПЗ. Верифікація та валідація ПЗ. Тестування ПЗ. Оптимізація коду та рефакторинг. Аспекти продуктивності ПЗ. Інтегровані середовища розробки ПЗ. Системи управління проектами. Системи управління версіями документів, архітектурні особливості. Інструменти автоматизації зборки проектів. Інструменти автоматизації процесів тестування.

Вибіркові компоненти ОПП
Вибірковий блок (за вибором університету)

Правова культура особистості. «Правова культура особистості» як навчальна дисципліна дозволить студентам виробити правове мислення і культурний стиль правомірної поведінки у повсякденному житті як у міжособистісних відносинах, так і при спілкування із представниками судових та правоохоронних органів. На вибір цього стилю впливають: 1) ступінь засвоєння і прояву цінностей правової культури суспільства; 2) специфіка професійної діяльності; 3) індивідуальна неповторність творчості кожної особистості та правові результати.

Діловий протокол та етика спілкування. Метою вивчення дисципліни є підвищення рівня загальномовної підготовки, комунікативної компетентності студентів, практичне оволодіння основами стилістики української мови, що забезпечить професійне спілкування на належному мовному рівні. Також розглянуто моральні й психологічні засади культури ділового спілкування та його техніку. Розкрито поняття етики, моралі, спілкування, моральної та психологічної культури ділового спілкування. Проаналізовано етико-психологічні проблеми ділового спілкування в нашому суспільстві з урахуванням науково-практичних висновків як вітчизняних, так і зарубіжних етиків та психологів, зокрема представників гуманістичної етики і гуманістичної психології. Висвітлено шляхи підвищення моральної та психологічної культури спілкування.

Технологія виробництва продукції рослинництва та тваринництва. Стан та основні напрями розвитку рослинництва в Україні; значення і біологічні особливості польових культур, видів і сортів сільськогосподарських рослин, їх використання, поширення та потенціал урожайності і продуктивності; сучасні технології вирощування високих, екологічно-чистих урожаїв сільськогосподарських культур у різних ґрунтово-кліматичних зонах України; шляхи і способи покращання якості сільськогосподарської продукції; заходи щодо недопущення втрат урожаю під час збирання. транспортування та зберігання; способи скорочення затрат праці на вирощування врожаю. Науково-теоретичні основи технологічних процесів. та оцінка продукції тварин. Ефективне здійснення селекційного процесу в бажаному напрямі та організація біологічно обґрунтованої і економічно доцільної технології виробництва, переробки і зберігання продукції тварин. Система практичних методів контролю цілісних комплексних процесів, на основі яких здійснюється технологія виробництва, переробки і зберігання продукції тварин. Принципи організації технологічних потоків переробки сировини.

Виготовлення м'ясної, рибної та молочної продукції, яєць різноцільового призначення.

Історія української державності. Мета дисципліні - розглянути теоретико-концептуальні проблеми української державності від витоків до сучасності. На основі наукової джерельної бази та новітніх досліджень. Осмислити ключові аспекти історії, національних та державотворчих процесів, основні етапи формування українського національно-визвольного руху, його конкретний зміст і форми. Визначити роль і місце в національному державотворенні видатних історичних осіб. Шляхом переосмислення та оновлення історичних знань, що є гарантією незворотності національно-державного відродження українського народу – сформувати всебічно розвинену та соціально активну особистість, з чіткою громадянською позицією.

Іноземна мова (англійська, німецька, французька, іспанська). Вивчення дисципліни розвиває у студентів комунікативну компетенцію, а саме використання навичок, умінь та знань з іноземної мови у процесі ділового спілкування з представниками інших країн з різноманітних питань, пов’язаних із бізнесом і ринком праці в галузі сільського господарства, підготовки до участі у міжнародних конференціях, проектах та дискусіях, а також проведення презентацій, письмового обміну діловою інформацією (офіційні та неофіційні листи, резюме різні види науково-дослідних статей і звітів), сприяючи, таким чином, різнобічному розвитку особистості студента та його соціалізації в іншомовному суспільстві.

Філософія. В курсі викладається система знань із таких розділів філософії як онтологія, гносеологія (теорія пізнання), соціальна філософія, історичні типи філософії, що розкривають сутність відношення “людина – світ” в його найосновніших проявах. Курс відзначається світоглядною орієнтацією, яка дозволяє синтезувати набуті знання з фахових та гуманітарних дисциплін у цілісне світосприймання – теоретичне підґрунтя університетського рівня підготовки фахівців.

Економіка та бізнес Економіка підприємства. Загальний менеджмент, функції і методи управління. Маркетинг: система маркетингу на підприємстві, методи дослідження ринків, маркетингове планування. Стратегічний менеджмент: модель, стратегії, технології стратегічного планування PEST. SWOT. BCG. SNW та інші. Фінансовий менеджмент. Бізнес-планування: розробка бізнес-плану, джерела інвестицій. Бухгалтерський обпік і оподаткування. Управлінський облік. Управління виробництвом. Прогнозування діяльності підприємства. Маркетинг. Управління продажами та ресурсами. Логістика.

Бюджетування та контролінг. Управління персоналом.

Інформаційні технології (частини 1 та 2). Предмет, методи і завдання дисципліни, теоретичні основи інформатики, системне забезпечення інформаційних процесів, програмні засоби роботи зі структурованими документами, мережні технології, застосування Internet в економіці, Основи Web-дизайну, організація комп'ютерної безпеки та захисту інформації, програмні засоби роботи з базами та сховищами даних, основи офісного програмування, експертні і навчальні системи, перспективи розвитку інформаційних технологій.

Фізичне виховання. Мета викладання дисципліни полягає у формуванні фізичної культури молодого фахівця і здатності реалізувати її в соціально- професійній підготовці та в сім'ї. Завданням вивчення дисципліни є зміцнення здоров'я студентів та розвиток фізичних здібностей, які відповідають професійній діяльності майбутнього фахівця.

2. ЦИКЛ СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ
Обов'язкові компоненти ОПП

Методи та засоби захисту інформації. Знайомство з основними фізичними принципами, методами та засобами захисту інформації та пошуку апаратури, яка призначається для знімання інформації. Вивчення методів та засобів несанкціонованого одержання інформації, а також створення протидії захисту інформації по каналах, на яких можливі її втрати.

Комп'ютерна логіка - частина 1. В першій частині курсу «**Комп'ютерна логіка**» розглядаються наступні теми: Основні положення та означення комп'ютерної логіки. Інформаційні основи комп'ютерної техніки, зокрема для завдань захисту інформації та кібербезпеки. Алгебра перемикальних функцій. Методи мінімізації перемикальних функцій. Синтез комбінаційних схем у різних елементних базисах. Основи теорії цифрових автоматів з пам'яттю.

Комп'ютерна логіка - частина 2. В другій частині курсу «**Комп'ютерна логіка**» розглядаються наступні теми: Методи синтезу цифрових автоматів з пам'яттю. Аналіз логічних схем та динамічних процесів в цифрових автоматах. Типові цифрові схеми комп'ютерів. Введення в теорію систем числення. Форми подання та кодування чисел в комп'ютерах. Операції з фіксованою комою. Операції з плаваючою комою. Синтез операційних автоматів. Цифрові автомати як основа побудови сучасних цифрових систем захисту інформації та кібербезпеки.

Комплексні системи захисту інформації. Вивчення організаційних та інженерно-технічних заходів, спрямованих на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу. Знайомство з базовими організаційними заходами для комплексних систем захисту інформації, а також інженерно-технічними заходами. Засвоєння функціональних можливостей та методів побудови комплексних систем захисту інформації, опановування необхідними прийомами та практичними навичками при налаштуванні та конфігуруванні сучасного мережевого обладнання.

Інформаційна безпека держави. Інформаційна безпека є однією із суттєвих складових частин національної безпеки країни. Дисципліна вивчає способи, методи, засоби, а також канали реалізації загроз національним інтересам на інформаційному рівні. Також вивчаються базові методи та засоби своєчасного виявлення, запобігання і нейтралізації загроз для інформаційної безпеки держави. Метою вивчення навчальної дисципліни «Інформаційна безпека держави» є формування знань про теоретичні основи інформаційної безпеки, особливості забезпечення інформаційної безпеки держави, правила відношення інформації до державної таємниці, конфіденційної інформації, що є власністю держави, недержавної конфіденційної і відкритої інформації що потребує захисту, шляхи побудови систем забезпечення інформаційної безпеки.

Організаційне забезпечення захисту інформації. Роль організаційного захисту інформації в системі заходів безпеки визначається своєчасністю та правильністю прийнятих управлінських рішень, способів і методів захисту інформації на основі чинних нормативно-методичних документів. Організаційні методи захисту передбачають проведення організаційно-технічних та організаційно-правових заходів, а так само включають в себе наступні принципи захисту інформації: науковий підхід до організації захисту інформації; планування захисту; керування системою захисту; безперервність процесу захисту інформації; мінімальна достатність організації захисту; системний підхід до організації та проектування систем та методів захисту інформації; комплексний підхід до організації захисту інформації; відповідність рівня захисту цінності інформації; гнучкість захисту; багатозональність захисту, що передбачає розміщення джерел інформації в зонах з контрольованим рівнем її безпеки; обмеження числа осіб, які допускаються до захищеної інформації; особиста відповідальність персоналу за збереження довіреної інформації.

Компонентна база та схемотехніка в системах захисту інформації - частина 1. Розглядаються наступні теми: Схемотехніка

типових вузлів і блоків. Основи комп’ютерної схемотехніки. Типові вузли і блоки цифрової техніки. Тригери. Регістри. Лічильники. Двійкові суматори. Декодери. Мультиплексори. Шифратори. Пристрої пам’яті. Оперативна пам'ять. Регістрова та буферна пам'ять. Постійна пам'ять. Схемотехніка арифметичних пристроїв. Різновиди суматорів. Структури арифметичних пристроїв різного призначення.

Компонентна база та схемотехніка в системах захисту інформації - частина 2. Розглядаються наступні теми: Різновиди та реалізація каналів передачі інформації, зокрема захищених. Схемотехніка систем захисту інформації на ВІС та НВІС. Схемотехніка ПЛІС.

Теорія ризиків інформаційної безпеки. Порушення основних властивостей інформації може стати серйозною загрозою для організацій в даний час. Інформацію важче контролювати та вона піддається великому числу загроз і уразливостей, в тому числі комп'ютерного шахрайства, шпигунству, саботажу, вандалізму, пожежі або повені. Інформаційні ресурси, як і матеріальні, володіють якістю та кількістю, мають собівартість і ціну. Оцінка ризиків є важливою частиною будь-якого процесу інформаційної безпеки. Її використовують для визначення масштабу загроз безпеці інформації та ймовірності реалізації загрози. Метою дисципліни “Теорія ризиків інформаційної безпеки” є вивчення процесу оцінки ризику та оцінювання ймовірності та потенційного збитку від виявлених загроз, а також розробки моделей оцінювання індивідуального рівня ризику кожного інформаційного активу.

Безпека інформації в інформаційно-комунікаційних системах. Навчальна дисципліна є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в області кібербезпеки. На базі здобутих знань та умінь фахівець зможе вирішувати професійні задачі, що базуються на сучасних технологіях та методах захисту інформації у сучасних інформаційно-комунікаційних систем та мереж. Метою викладання дисципліни є розкриття сучасних методів захисту інформації в комп’ютерних системах та мережах і ознайомлення з особливостями їх апаратної та програмної реалізацій. Дисципліна передбачає вивченні: видів загроз інформації в комп’ютерних системах та мережах; основних протоколів безпеки; принципів функціонування систем захисту; основних програмних і апаратних засобів захисту інформації в комп’ютерних системах та мережах; методів несанкціонованого зняття та навмисного пошкодження інформації та засоби протидії цим спробам.

Архітектура та програмування мікроконтролерів - частина 1. Метою викладання навчальної дисципліни (Частина-1) є ознайомлення студентів з сучасними засобами розробки вбудованого програмного

забезпечення для мікроконтролерів. Вивчення архітектури сучасних мікроконтролерів. Вивчення можливостей та сфер застосування мікроконтролерів в системах захисту інформації та кібербезпеки.

Архітектура та програмування мікроконтролерів - частина 2. Метою викладання навчальної дисципліни (Частина-2) є надбання досвіду з розробки програмного забезпечення для сучасних мікроконтролерів. Основними завданнями вивчення дисципліни є надбання навичок роботи з технічною документацією на сучасні мікроконтролери та електронні компоненти в системах захисту інформації та кібербезпеки. Надбання навичок з розробки вбудованого програмного забезпечення.

Технології захисту інформації. Дисципліна сприяє підготовці майбутніх фахівців до ефективного використання сучасних інформаційних технологій в процесі розв'язування завдань безпеки даних та захисту цифрової інформації. Завдання дисципліни "Технології захисту інформації": засвоєння знань, умінь і навичок з основ захисту інформації і набуття навичок практичного їх застосування при роботі з сучасним прикладним програмним забезпеченням; методики побудови захисту інформації в інформаційних системах; сучасні засоби взаємодії людини з апаратним і програмним забезпеченням; основ крипто захисту даних; методики захисту важливої інформації від несанкціонованого доступу.

Основи криптоаналізу. Дисципліна має своєю метою дати студентам знання в галузі теоретичної криптографії та криптоаналізу. Дисципліна знайомить з основними принципами роботи крипто аналітиків, математичними моделями джерел інформації, поняттями теоретичної та практичної секретності, а також практичними прийомами в роботі криптоаналітика.

Системне програмування - частина 1. Метою першої частини курсу «Системне програмування» є формування у студентів знань та вмінь роботи із мовою assembler, як засобом ефективного програмування, вивчення архітектури і системи команд базового процесора, створення підпрограм на мові assembler.

Системне програмування - частина 2. Метою другої частини дисципліни «Системне програмування» є формування у студентів знань та вмінь стосовно засобів побудови системних програм, програмування системних програм за допомогою мов С та С++. При вивченні дисципліни охоплюються, зокрема, наступні питання: технології розробки багатомодульних системних програм, використання програмних бібліотек, обробка структур даних в системних програмах. Питання

оптимізації коду системних програмних продуктів для завдань захисту інформації та кібербезпеки.

Комп'ютерні мережі - частина 1. Метою першої частини дисципліни «Комп'ютерні мережі» є формування у студентів знань та базових вмінь, які стосуються теоретичних та практичних аспектів, а також методології проектування, побудови та використання комп'ютерних мереж.

Комп'ютерні мережі - частина 2. Метою другої частини дисципліни «Комп'ютерні мережі» є вивчення студентами архітектури сучасних комп’ютерних мереж, програмного забезпечення для конфігурації мереж, набуття практичних навичок аналізу захищеності мереж від несанкціонованого доступу до інформації.

Основи криптографічного та стеганографічного захисту інформації. Дисципліна знайомить студентів з класичними та сучасними симетричними криптографічними системами, криптографією з відкритим ключем, різноманітними криптографічними протоколами та їх застосуванням, а також з новими перспективними напрямками розвитку криптології. Дисципліна має своєю метою дати студентам знання в галузі теоретичної криптографії та стеганографії. Дисципліна знайомить з основними принципами роботи криптографів, математичними моделями джерел інформації. Конкретні типи алгоритмів шифрування та криптографічних перетворень розглядаються відповідно до їх класифікації на класичні схеми, системи потокового шифрування, системи блокового шифрування та системи захисту інформації з відкритим ключем. Багато уваги приділяється криптографічним протоколам та їх застосуванням у захисті сучасних інформаційних технологій.

Комп'ютерні системи. Дисципліна присвячена розгляду наступних питань: Структура, принципи створення і класифікація комп'ютерних систем (КС). Предмет, завдання та методи теорії КС. Обчислювальні процеси в КС та їх моделі. Планування робіт в КС. Метрики КС: продуктивність, ефективність, надійність. Структурна організація КС різних поколінь. Класифікація паралельних КС. КС з фіксованою системою зав’язків. КС з реконфігурованою системою зав’язків. Організація пам’яті в КС. Організація вводу-виводу даних в КС. Організація передачі даних в КС. КС класу SISD. КС класу SIMD: матричні, векторні, асоціативні. КС класу MISD: конвеєрні комп’ютерні системи. КС класу MIMD: мультипроцесорні, мультикомп’ютерні, системи з неоднорідним доступом до оперативної пам’яті, кластерні системи, GRID системи. Комп’ютерні системи з нетрадиційною архітектурою. Інтерфейси КС. Основні поняття відмовостійкості КС. Структурні аспекти

побудови відмовостійких КС. Місце комп'ютерних систем в інтегрованих системах проектування, виробництва і експлуатації. Зв'язок комп'ютерних систем з іншими автоматизованими системами. Організація і методика по-будови сучасних програмно-технічних комплексів, зокрема пов’язаних із захистом інформації та кібербезпекою. Приклади сучасних систем проектування та інженерного аналізу. Структура систем інженерного аналізу для захисту інформації та кібербезпеки. Види комп'ютерних систем для захисту інформації та забезпечення кібербезпеки об’єктів інформатизації.

Захист інформації в компютерних системах. В дисципліні розглядаються основні принципи і рішення в області проектування та налагодження систем інформаційної безпеки та кібербезпеки в спеціалізованих комп’ютерних та робото технічних системах і мережах. Мета дисципліни – отримання студентами необхідних знань щодо кібернетичних загроз спеціалізованим комп’ютерним та робото технічним системам і мережам. Знайомство з основними методами, принципами, алгоритмами захисту інформації в комп’ютерних системах з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення загроз та кібератак зі сторони потенційних порушників. Під час вивчення дисципліни передбачається формування у студентів певних знань та вмінь з теорії та практики захисту інформації та інформаційної безпеки в спеціалізованих комп’ютерних та робото технічних системах і мережах.

Системне програмне забезпечення-частина 1. Мета вивчення дисциплін „Системне програмне забезпечення” (Частина 1) - підготовка спеціалістів до ефективного застосування сучасної комп’ютерної техніки з метою її оптимального використання в завданнях захисту інформації та кібербезпеки, здобуття навичок роботи з операційними системами Windows для встановлення і повноцінного адміністрування ОС на персональних комп’ютерах та серверах, в роботі з пакетами прикладних програм та додаткових програмних оболонок, тощо.

Системне програмне забезпечення-частина 2. В частині 2 курсу „Системне програмне забезпечення” розглядаються теми, які пов’язані із здобуттям навичок роботи з операційними системами Unix/Linux для встановлення і повноцінного адміністрування ОС на персональних комп’ютерах та серверах.

Вибіркові компоненти ОПП

Вибірковий блок 1 «Безпека інформаційно-комунікаційних систем»

Управління доступом. Сучасні інформаційні та комп’ютеризовані системи уразливі до ряду мережних загроз, які можуть бути результатом

реалізації несанкціонованого доступу, а також розкриття або модифікації інформації. Щоб захистити відповідні інформаційні ресурси від кіберзагроз, необхідно застосовувати цілеспрямовані заходи управління доступом. Вивченню та засвоєнню керівних та загальних принципів побудови, реалізації, підтримки та покращення системи керування доступом та захистом інформації присвячена ця дисципліна. Студенти здобувають практичні навички з планування та розроблення ефективної системи управління доступом, яка забезпечує керування й контроль доступу, розробку й обслуговування апаратно-програмних систем та мереж; керування безперервністю бізнес-процесів та оптимізацію управлінських процесів. Студенти навчаються ідентифікувати специфічні ризики порушення безпеки, які загрожують ресурсам організації та для яких оцінюють уразливість, ймовірність її виникнення та потенційний вплив; розробляти політику безпеки; здійснювати організацію керування активами й ресурсами з метою підвищення ефективності функціонування і захищеності комп'ютерних систем.

Системний аналіз. Мета: виробити навички системного мислення у студентів і підготувати їх до рішення практичних задач аналізу і синтезу систем захисту інформації, інформаційної та (або) кібербезпеки. Завдання: вивчення методології системного підходу, широко застосовуваного при вирішенні глобальних і спеціальних проблем, таких як моніторинг, керування технологічними процесами, інформаційними системами, технічне діагностування, і т.п.

Об'єктно-орієнтоване програмування. Класи та об'єкти в C++. Поля та методи класу. Варіанти синтаксису та структури опису класу. Інкапсуляція через специфікатори доступу. Звернення до об'єкту через покажчик. Конструктор класу. Стандартні списки ініціалізації. Деструктори. Конструктор копіювання. Конструктор переносу. Статичні члени класу, константи. Дружні функції, дружні класи. Вкладені класи. Успадкування як ключовий момент ООП. Сценарії використання. Делегування та успадкування конструкторів). Зміни рівня доступу до членів класу при різних сценаріях успадкування. Множинне успадкування. Поняття поліморфізму, переваги та недоліки, альтернативи. Віртуальні функції як основа поліморфізму в C++. Дослідження реалізації поліморфізму в C++. Абстрактні класи. Концепція інтерфейсу в ООП. Віртуальні деструктори. Обробка виключень. Виключення-об'єкти, варіанти перехоплення, використання поліморфізму. Обмеження виключень. Поняття шаблону в C++ (template). Шаблонні функції та шаблонні класи. Елементи метапрограмування.

Ліцензування і сертифікація засобів захисту інформації. Метою вивчення дисципліни є формування знань про організацію системи

державного ліцензування в галузі захисту інформації, сертифікації та атестації об'єктів захисту інформації, а також організації заходів з інформаційної безпеки на об'єкті інформатизації та про їх правове забезпечення. Дисципліна розкриває основні поняття та види інформації, що захищається відповідно до законодавства України, дає знання про систему захисту державної таємниці, конфіденційної інформації, формує професійні компетенції, необхідні для здійснення професійної діяльності. Завдання вивчення дисципліни: вивчення інформаційного законодавства України і міжнародного законодавства в області захисту інформації; формування знань в області організації державного ліцензування в області захисту інформації; розвиток навичок організації системи сертифікації і атестації об'єктів інформатизації.

Захищені мережеві технології обробки інформації. Метою вивчення дисципліни є формування знань про основні методи та засоби захисту інформаційних ресурсів, зокрема, технології ідентифікації, аутентифікації та управління доступом у комп’ютерних мережах та системах; принципи багаторівневого захисту корпоративної мережі, інтегрованої з мережами загального доступу, наприклад, Інтернет; міжмережеві екрани; концепція побудови віртуальних захищених мереж VPN.

Безпека при експлуатації і обслуговуванні IT систем. Вивчаються теорія надійності і ефективності комп’ютерних систем та програмних засобів з погляду відновлювальних та невідновлювальних об’єктів, зокрема після подій пов’язаних с кібер інцидентами. Розглядаються показники безвідмовності, ремонтопридатності, довговічності та зберігаємості елементів та систем, комплексні показники надійності. Вивчаються методи побудов структурних схем надійності та дерев відмов. Розглядаються методи оцінювання надійності систем без відновлення та з відновленням, з резервуванням. Вивчаються основні поняття технічної діагностики, принципи організації систем технічної діагностики та використання автоматизованих систем діагностування.

Крос-платформне програмування. Метою викладання навчальної дисципліни «Крос-платформне програмування» є забезпечення отримання студентами теоретичних знань і практичних навичок компонентного програмування, принципів технології розробки крос-платформних програмних систем, принципів використання засобів крос-платформного програмування. Теми: архітектура та стандарти компонентних моделей, комунікаційних засобів і розподілених обчислень; стратегії інтеграції програмних компонентів; основні платформи проміжного рівня та компонентні моделі; формальні та візуальні методи конструювання компонентів; розробка вимог та специфікацій компонентів інформаційних систем і об'єктів професійної

діяльності; проектування компонентів програмного забезпечення; проектування людино-машинного інтерфейсу інформаційних систем; інтеграція компонентів в систему.

Безпека розробки і підтримки додатків. Мета дисципліни - вивчення засобів та методів захисту та безпеки інформації для безперебійного та ефективного використання програм та даних у різних комп'ютеризованих системах, сучасних методів розробки та підтримки даних, перспективних алгоритмічних методів захисту програм та даних.

Адміністрування комп'ютерних мереж. Мета дисципліни вивчення основ теорії та отримання практичних навиків мережевого адміністрування інформаційної системи організації – управління мережевими вузлами, мережевими протоколами, службами каталогів, мережевими службами, управління файловими ресурсами системи, правами доступу до ресурсів, пристроями друку, системами резервного копіювання та відновлення інформації, здійснення моніторингу мережевих пристроїв і служб.

Управління проектами захисту інформації. Мета дисципліни є формування у студентів цілісної системи знань щодо набуття навичок управління проектами захисту інформації на підприємстві, в установі, у галузі, регіоні та країні. Під час курсу студенти знайомляться із: сучасними методами та технологіями управління проектами захисту інформації та місцем управління проектом у загальній системі управління інформаційною безпекою. Вивчаються: історію розвитку, накопичений досвід та стан управління проектами захисту інформації в Україні та світі; зміст та структуру проекту захисту інформації, його життєвий цикл; теорія організації управління проектом захисту інформації. Результатом вивчення дисципліни є формування у майбутніх фахівців належної компетентності з ефективного управління проектами захисту інформації в організаціях.

Програмування в середовищі сучасних ОС. Розглядаються наступні теми: програмування у середовищі сучасних ОС (Linux, MacOS, Android), з урахуванням їх структури, функцій, позицій стосовно багатопоточної обробки даних; багатопоточне програмування на мовах високого рівня, із залученням сучасних інтегрованих засобів розробки.

Вибірковий блок 2 «Управління інформаційною безпекою»

Технології комп'ютерного проектування систем захисту інформації. Метою вивчення дисципліни є формування знань про основні методи та технології автоматизованого моделювання, проектування та дослідження систем захисту інформації. Вивчаються технології проектування комп'ютеризованих систем кібербезпеки та

захисту інформації для реальних об’єктів захисту. Вивчаються об’єктно-орієнтовне проектування та конструювання систем кібербезпеки та захисту інформації, компоненти та складові P-CAD, приклади синтезу систем захисту інформації у P-CAD.

Системи прийняття рішень в завданнях захисту інформації. Мета дисципліни - ознайомлення із загальнодержавними програмами та напрямками інформатизації систем управління інформаційною безпекою та кібербезпекою, формування системного підходу до аналізу сучасного стану і тенденцій розвитку систем підтримки прийняття рішень в завданнях кібербезпеки об’єктів інформатизації, вивчення методики визначення стратегічної та оперативної спрямованості систем підтримки прийняття рішень в завданнях захисту інформації та кібербезпеки, вивчення теоретичних аспектів запровадження в організації систем підтримки прийняття рішень, зокрема з завдані захисту інформації та формування комплексних систем захисту інформації на базі сумісних апаратно-програмних комплексів та використання технологій штучного інтелекту.

Сучасні технології програмування. В результаті вивчення даної дисципліни студент набуває знання та практичні навички використання сучасних технологій програмування в середовищі операційних систем Windows та Linux. Вивчаються завдання об'єктно-орієнтованого програмування (ООП), використання потоків, робота з DLL для забезпечення захисту та кібербезпеки об’єктів інформатизації.

Безпека безпровідних, мобільних та хмарних технологій. Сучасні інформаційно-комунікаційні технології передбачають використання технологій віртуалізації технологій серверних систем, комунікаційних засобів для розподілених обчислень та розроблення програмно апаратних рішень центрів обробки даних. Для управління кібербезпекою неоднорідних обчислювальних ресурсів у віддаленому режимі потрібні програмні та апаратні рішення для захищених впровадження систем віртуалізації, а також віддалених сервісних функцій, що загалом створює можливості для організації та застосування технологій безпровідних, мобільних і хмарних обчислень. Метою викладання навчальної дисципліни є формування теоретичних знань і придбання практичних умінь і навичок з питань використання технологій захищених розподілених обчислень, віртуалізації серверних систем, проектування захищених корпоративних обчислювальних систем із застосуванням безпровідних, мобільних і хмарних обчислень.

Основи аудиту інформаційної безпеки. Дисципліна «Основи аудиту інформаційної безпеки» вивчає системний процес одержання об'єктивних якісних і кількісних оцінок поточного стану безпеки

інформаційної системи або інформаційно-телекомунікаційної системи, а також дозволяє виконувати комплексну оцінку рівня інформаційної безпеки об’єктів інформатизації Замовника з урахуванням трьох основних факторів: персоналу, процесів та технологій. Порівняльний аналіз поточного стану інформаційної системи, що визначається за підсумками анкетування, з тестовою моделлю вимог стандарту ISO 27001.

Необхідність проведення регулярного аудиту інформаційної безпеки полягає в здійсненні оцінки реального стану захищеності ресурсів ІС та/або ІТС та їх спроможності протистояти зовнішнім і внутрішнім загрозам інформаційної безпеки, які постійно змінюються та адаптуються. Державне підприємство "Українські спеціальні системи" пропонує провести аудит інформаційної безпеки на об’єктах інформаційної діяльності Замовника, з метою визначення стану захищеності ІС та/або ІТС, засобами якої обробляється конфіденційна чи інша критична інформація Замовника, а також відповідності ІС та/або ІТС стандартам та нормативним документам в державному або комерційному та секторі.

Архітектура і моделі безпеки. Курс базується на сучасних практиках в сфері кібербезпеки та інформаційної безпеки, зокрема на Business Model for Information Security (BMIS). Під час вивчення дисципліни детально розглядаються та аналізуються компоненти BMIS (організація, люди, технології, процеси) та динамічні взаємозв’язки між ними (інформаційні технології, архітектура систем різного призначення, культура, управління, людський фактор). Моделі ідентифікації поточного стану інформаційної та кібербезпеки. Методи та моделі оцінки інформаційної безпеки організації, зокрема Threat and Risk Assessment (TRA). Підходи, щодо визначення факторів, які впливають на стан інформаційної безпеки; методи визначення ступеню взаємозв’язків між факторами та їх влив на стан інформаційної та кібербезпеи підприємства. Розглядаються можливі підходи до оцінки адекватності отриманих моделей інформаційної та кібербезпеки; Моделювання можливих сценаріїв зміни інформаційної та кібербезпеки організації.

Програмування на мові Java. Метою дисципліни є формування у студентів практичних навичок створення застосунків на мові Java. Задачею дисципліни є - ознайомлення студентів із особливостями програмування на мові Java та набуття досвіду у створенні Java застосунків. Предмет дисципліни – принципи створення різних типів застосувань на Java. По закінченні вивчення дисципліни студенти повинні отримати певний рівень знання про мову програмування Java, розуміти особливості створенні Java застосунків. Студенти мають вміти застосовувати засоби отримані навички для вирішення задач проектування кроссплатформених застосувань та розробки Web-

застосувань із використанням аплетів та сервлетів.

Проведення розслідувань інцидентів інформаційної безпеки. Для обробки подій та інцидентів інформаційної безпеки (ІБ) необхідно організувати процес реагування на інциденти. Дисципліна «Проведення розслідувань інцидентів інформаційної безпеки», відповідно знайомить студентів: із методологією організації процесу реагування на інциденти ІБ; методами забезпечення координації реагування на інцидент; засобами підтвердження/спростування факту виникнення інциденту ІБ; методами мінімізації порушень порядку роботи і пошкодження даних ІТ-системи, методами відновлення в найкоротші терміни працездатності організації при її порушенні в результаті інциденту та мінімізації наслідків порушення конфіденційності, цілісності і доступності інформації ІТ-систем. Також вивчають основні підходи до створення умов захисту репутації організації та її ресурсів; швидкого виявлення та/або попередження подібних інцидентів в майбутньому; методів навчання персоналу компанії діям з виявлення, усунення наслідків і запобігання інцидентів ІБ та своєчасного інформування керівництва про стан інформаційної безпеки.

Управління веб-контентом. Дисципліна розглядає системи електронного документообігу та системи управління корпоративним web контентом, які забезпечують ефективне управління інформацією за рахунок її надійного зберігання та організації доступу до неї. Ці системи є основою впровадження стратегій управління корпоративним контентом та управління знаннями на підприємстві, що забезпечує його інноваційний розвиток.

Продукти та послуги інформаційної безпеки. Мета дисципліни «Продукти та послуги інформаційної безпеки» є формування у студентів знань та вмінь для проведення тесту на проникнення в інформаційну систему, який є найкращим способом, що дозволяє оцінити захищеність інформаційної системи в цілому, виявити окремі уразливості і перевірити надійність чинних механізмів захисту інформаційної системи від несанкціонованого впливу, використовуючи різні моделі порушників. Під час вивчення дисципліни вивчаються: методи оцінки поточного стану інформаційної безпеки; методика виявлення уразливостей інформаційної системи з їх ранжуванням за ступенем критичності; вимоги міжнародних стандартів та законодавства; методика розробки рекомендацій щодо підвищення ефективності захисту; методика надання клієнту незалежної оцінки обраних заходів інформаційного захисту; методологія підготовки даних для проведення комплексного аудиту інформаційної безпеки об’єкту інформатизації.

Розробка додатків в сучасних ОС. Метою дисципліни «Розробка додатків в сучасних ОС» є формування у студентів знань та вмінь

програмування у середовищі сучасних ОС (Linux, MacOS, Android), з урахуванням їх структури, функцій, позицій стосовно багатопоточної обробки даних. При вивченні дисципліни студенти одержують навички багатопоточного програмування на мовах високого рівня, із залученням сучасних інтегрованих засобів розробки, ознайомлюються із аспектами використання контейнерів даних, одержують, зокрема, навички створення веб-додатків.

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 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	ОК23
КЗ1		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
КЗ2				+		+	+	+	+	+	+	+		+	+		+	+	+	+		+	+
КЗ3			+		+					+		+		+								+	+
КЗ4				+		+	+	+	+	+	+	+		+	+		+	+	+	+			+
КЗ5																							
КЗ6																							
КЗ7							+																
КЗ8	+	+	+	+	+					+	+		+		+			+		+			
ФК1							+		+														
ФК2				+		+						+					+		+	+			
ФК3								+		+		+	+	+		+	+		+	+	+	+	
ФК4									+														
ФК5				+		+		+	+		+	+		+			+			+			
ФК6									+								+			+	+	+	
ФК7				+				+	+			+	+	+			+						
ФК8																							
ФК9									+														
ФК10				+				+						+	+					+			+
ФК11				+				+									+						
ФК12				+																+			
ФК13																							
ФК14																							
ФК15																							

	ВУ1	ВУ2	ВУ3	ВУ4	ВУ5	ВУ6	ВУ7	ВУ8	ВУ9	ВБ1.1	ВБ1.2	ВБ1.3	ВБ1.4	ВБ1.5	ВБ1.6	ВБ1.7	ВБ1.8	ВБ1.9	ВБ1.10	ВБ1.11	ВБ1.12	ВБ1.13	
К31	+	+	+		+		+	+		+	+	+	+					+	+	+	+	+	
К32								+		+	+	+	+	+	+	+	+	+	+	+	+	+	
К33		+			+																		
К34										+	+	+	+	+	+	+	+	+	+	+	+	+	
К35					+																		
К36	+	+		+		+																	
К37	+	+		+		+	+		+														
К38						+					+	+				+						+	
ФК1	+							+					+										
ФК2														+	+					+			
ФК3										+				+	+		+		+	+		+	
ФК4							+																
ФК5										+				+	+				+	+			
ФК6														+	+				+	+			
ФК7														+	+				+	+			
ФК8										+			+										
ФК9										+				+					+	+			
ФК10														+	+					+			
ФК11														+	+				+	+			
ФК12																			+				
ФК13																							
ФК14																							
ФК15																		+	+				

	ВБ2.1	ВБ2.2	ВБ2.3	ВБ2.4	ВБ2.5	ВБ2.6	ВБ2.7	ВБ2.8	ВБ2.9	ВБ2.10	ВБ2.11	ВБ2.12	ВБ2.13
ЗК1	+	+	+	+					+	+	+	+	+
ЗК2	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК3													
ЗК4	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК5													
ЗК6													
ЗК7													
ЗК8			+				+						+
ФК1												+	
ФК2						+							
ФК3	+			+						+	+		+
ФК4				+				+			+	+	
ФК5				+									
ФК6				+									
ФК7				+	+			+					
ФК8					+			+					
ФК9											+		
ФК10				+									
ФК11													
ФК12					+			+					
ФК13													
ФК14													
ФК15													

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	ОК23
ПРН1																							
ПРН2																							
ПРН3			+		+					+		+		+				+				+	+
ПРН4					+					+		+		+				+				+	+
ПРН5				+				+	+														
ПРН6				+					+		+	+								+			
ПРН7							+		+														
ПРН8							+		+														
ПРН9							+		+														
ПРН10					+	+							+						+				
ПРН11						+											+		+				
ПРН12				+																+			
ПРН13				+		+		+			+	+		+			+		+				
ПРН14								+				+		+		+	+			+	+		
ПРН15			+													+					+		+
ПРН16						+																	
ПРН17								+				+	+				+		+				
ПРН18								+		+											+		
ПРН19				+							+				+			+		+			
ПРН20																					+		
ПРН21																							
ПРН22																							
ПРН23																							

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23
ПРН24																							
ПРН25																							
ПРН26																							
ПРН27				+							+						+						
ПРН28																							
ПРН29											+												
ПРН30											+												
ПРН31				+																+			
ПРН32								+	+		+										+		
ПРН33											+												
ПРН34									+														
ПРН35						+																	
ПРН36								+															
ПРН37								+															
ПРН38								+															
ПРН39									+														
ПРН40								+															
ПРН41									+														
ПРН42									+														
ПРН43							+																
ПРН44											+												
ПРН45											+												
ПРН46											+												
ПРН47															+			+					

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23
ПРН48															+			+					
ПРН49				+																+			
ПРН50				+				+				+								+			
ПРН51								+				+											
ПРН52								+				+											
ПРН53																					+		
ПРН54																							
ПРН55	+	+																					
ПРН56					+					+													

	ВУ1	ВУ2	ВУ3	ВУ4	ВУ5	ВУ6	ВУ7	ВУ8	ВУ9	ВБ1.1	ВБ1.2	ВБ1.3	ВБ1.4	ВБ1.5	ВБ1.6	ВБ1.7	ВБ1.8	ВБ1.9	ВБ1.10	ВБ1.11	ВБ1.12	ВБ1.13
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																						
ПРН31																						
ПРН32																						
ПРН33																						

	ВУ1	ВУ2	ВУ3	ВУ4	ВУ5	ВУ6	ВУ7	ВУ8	ВУ9	ВБ1.1	ВБ1.2	ВБ1.3	ВБ1.4	ВБ1.5	ВБ1.6	ВБ1.7	ВБ1.8	ВБ1.9	ВБ1.10	ВБ1.11	ВБ1.12	ВБ1.13
ПРН34																						
ПРН35																						
ПРН36															+							
ПРН37															+							
ПРН38															+							
ПРН39													+									
ПРН40															+							
ПРН41																						
ПРН42																						
ПРН43																						
ПРН44																						
ПРН45																						
ПРН46																						
ПРН47																						
ПРН48																						
ПРН49															+							
ПРН50														+	+							
ПРН51															+	+						
ПРН52																						
ПРН53																	+					
ПРН54	+	+		+																		
ПРН55																						
ПРН56																						

	ВБ2.1	ВБ2.2	ВБ2.3	ВБ2.4	ВБ2.5	ВБ2.6	ВБ2.7	ВБ2.8	ВБ2.9	ВБ2.10	ВБ2.11	ВБ2.12	ВБ2.13
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													
ПРН31													
ПРН32													
ПРН33													
ПРН34													
ПРН35													
ПРН36													
ПРН37													
ПРН38													
ПРН39					+								
ПРН40													
ПРН41					+							+	
ПРН42								+					

	ВБ2.1	ВБ2.2	ВБ2.3	ВБ2.4	ВБ2.5	ВБ2.6	ВБ2.7	ВБ2.8	ВБ2.9	ВБ2.10	ВБ2.11	ВБ2.12	ВБ2.13
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

НАВЧАЛЬНИЙ ПЛАН
підготовки фахівців 2019 року вступу

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

ГРАФІК НАВЧАЛЬНОГО ПРОЦЕСУ
підготовки фахівців першого (бакалаврського) рівня вищої освіти 2019 року вступу
Освітньо-професійна програма «Кібербезпека»

	2019 рік																	2020 рік								
	Вересень				30	Жовтень			28	Листопад				Грудень				30	Січень			27	Лютий			
	2 7	9 14	16 21	23 28	IX 5 X	7 12	14 19	21 26	X 2 XI	4 9	11 16	18 23	25 30	2 7	9 14	16 21	23 28	XII 4 I	6 11	13 18	20 25	I 1 II	3 8	10 15	17 22	24 29
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
I																										
II																										
III																										
IV																										

	2020 рік																									
	Березень				30	Квітень			27	Травень				Червень				29	Липень			27	Серпень			
	2 7	9 14	16 21	23 28	III 4 IV	6 11	13 18	20 25	IV 2 V	4 9	11 16	18 23	25 30	1 6	8 13	15 20	22 27	VI 4 VII	6 11	13 18	20 25	VII 1 VIII	3 8	10 15	17 22	24 29
	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																										
II																										
III																										
IV																										

Умовні позначення:

	-	теоретичне навчання
:	-	екзаменаційна сесія
-	-	канікули
О	-	навчальна практика
Х	-	виробнича практика
О	-	навчальна практика
//	-	державна атестація

ІІ. ПЛАН НАВЧАЛЬНОГО ПРОЦЕСУ

№ п.п.	Дисципліни	Загальний обсяг		Форми контролю знань (за семестрами)			Аудиторні заняття				Самостійна робота	Практична підготовка		Розподіл тижневих годин за курсами та семестрами							
								у тому числі						I курс		II курс		III курс		IV курс	
														Семестри							
														1	2	3	4	5	6	7	8
														Кількість тижнів у семестрі							
		Годин	Кредитів	Іспит	Залік	Курсова робота (проект)	**Всього**	лекції	лабораторні	практичні		Навч. практика	Виробн. практика	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**12**
1. ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ																					
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						
ОК3.01	Програмування - частина 1	180	6		1		90	30	60		90			6							
ОК3.02	Програмування - частина 2	150	5	2		2,КР	75	30	45		75				5						
Всього		**870**	**29**	**3**	**2**		**435**	**180**	**165**	**90**	**435**			**12**	**17**						
Вибіркові компоненти ОПП																					
Вибірковий блок (за вибором університету)																					
ВУ1	Правова культура особистості	120	4	7			30	15		15	90									2	
ВУ2	Діловий протокол та етика спілкування	120	4	1			60	30		30	60			4							
ВУ3	Технології виробництва продукції рослинництва та тваринництва	120	4	4			60	30		30	60						4				
ВУ4	Історія української державності	120	4	1			30	15		15	90			2							
ВУ5.1	Іноземна мова - частина 1	30	1		1		30			30				2							
ВУ5.2	Іноземна мова - частина 2	60	2	2			30			30	30				2						
ВУ5.3	Іноземна мова - частина 3	60	2		3		30			30	30					2					
ВУ5.4	Іноземна мова - частина 4	30	1	4			30			30							2				
ВУ6	Філософія	120	4	5			60	30		30	60							4			
ВУ7	Економіка та бізнес	120	4	7			30	15		15	90									2	
ВУ8.1	Інформаційні технології - частина 1	90	3		1		60	30	30		30			4							
ВУ8.2	Інформаційні технології - частина 2	90	3	2			60	30	30		30				4						
ВУ9.1	Фізичне виховання - частина 1	30	1		1		30			30				2							
ВУ9.2	Фізичне виховання - частина 2	30	1		2		30			30					2						
ВУ9.3	Фізичне виховання - частина 3	30	1		3		30			30						2					
ВУ9.4	Фізичне виховання - частина 4	30	1		4		30			30							2				
Всього		**1080**	**36**	**9**	**7**		**630**	**195**	**60**	**375**	**570**			**14**	**8**	**4**	**8**	**4**		**4**	
2. ЦИКЛ СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ																					
Обов'язкові компоненти ОПП																					
ОК4	Методи та засоби захисту	150	5	3			75	45	30		75					5					

№ п.п.	Дисципліни	Загальний обсяг		Форми контролю знань (за семестрами)			Аудиторні заняття				Самостійна робота	Практична підготовка		Розподіл тижневих годин за курсами та семестрами							
								у тому числі						I курс		II курс		III курс		IV курс	
														Семестри							
														1	2	3	4	5	6	7	8
														Кількість тижнів у семестрі							
		Годин	Кредитів	Іспит	Залік	Курсова робота (проект)	**Всього**	лекції	лабораторні	практичні		Навч. практика	Виробн. практика	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**12**
	інформації																				
ОК5.1	Комп'ютерна логіка - частина 1	120	4	2			75	30	45		45				5						
ОК5.2	Комп'ютерна логіка - частина 2	180	6	3		3,КП	75	30	45		105					5					
ОК6	Комплексні системи захисту інформації	120	4	4			60	30	30		60						4				
ОК7	Інформаційна безпека держави	120	4	1			60	30	30		60			4							
ОК8	Основи технічного захисту інформації	120	4	4			60	30	30		60						4				
ОК9	Організаційне забезпечення захисту інформації	180	6	3			75	30	45		105					5					
ОК10.1	Компонентна база та схемотехніка в системах захисту інформації - частина 1	180	6	3			75	30	45		105					5					
ОК10.2	Компонентна база та схемотехніка в системах захисту інформації - частина 2	120	4	4		4,КП	60	30	30		60						4				
ОК11	Теорія ризиків інформаційної безпеки	120	4	4			60	30		30	60						4				
ОК12	Безпека інформації в інформаційно-комунікаційних системах	120	4	6		6,КР	45	15	30		75								3		
ОК13.1	Архітектура та програмування мікроконтролерів - частина 1	90	3		4		60	30	30		30						4				
ОК13.2	Архітектура та програмування мікроконтролерів - частина 2	150	5	5			60	30	30		90							4			
ОК14	Технології захисту інформації	120	4	7		7,КП	60	30	30		60									4	
ОК15	Основи криптоаналізу	120	4	6			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			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	150	5	7			60	30	30		90									4	
ОК18	Основи криптографічного та стеганографічного захисту інформації	120	4	5		5,КР	60	30	30		60							4			
ОК19	Комп'ютерні системи	90	3	6			60	30	30		30								4		

№ п.п.	Дисципліни	Загальний обсяг		Форми контролю знань (за семестрами)			Аудиторні заняття				Самостійна робота	Практична підготовка		Розподіл тижневих годин за курсами та семестрами							
								у тому числі						I курс		II курс		III курс		IV курс	
														Семестри							
														1	2	3	4	5	6	7	8
														Кількість тижнів у семестрі							
		Годин	Кредитів	Іспит	Залік	Курсова робота (проект)	**Всього**	лекції	лабораторні	практичні		Навч. практика	Виробн. практика	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**12**
ОК20	Захист інформації в компютерних системах	150	5	8			72	36	36		78										6
ОК21.1	Системне програмне забезпечення-частина 1	90	3	6			60	30	30		30								4		
ОК21.2	Системне програмне забезпечення-частина2	150	5	7			60	30	30		90									4	
ОК22	Проектно-технологічна практика	180	6									180									
ОК23	Підготовка і захист кваліфікаційної роботи	210	7									210									
Всього		**3450**	**115**	**22**	**2**		**1497**	**711**	**756**	**30**	**1563**	**390**		**4**	**5**	**20**	**20**	**11**	**23**	**12**	**6**
Загальний обсяг обов'язкових компонентів		**4320**	**144**	**25**	**4**		**1932**	**891**	**921**	**120**	**1998**	**390**		**16**	**22**	**20**	**20**	**11**	**23**	**12**	**6**
Вибіркові компоненти ОПП																					
Вибірковий блок 2 (за вибором студента)																					
Вибірковий блок 1 «Безпека інформаційно-комунікаційних систем»																					
ВБ1.1	Управління доступом	120	4	5			60	30	30		60							4			
ВБ1.2	Системний аналіз	120	4	5			45	15	30		75							3			
ВБ1.3	Об'єктно-орієнтоване програмування	150	5	5			60	30	30		90							4			
ВБ1.4	Ліцензування і сертифікація засобів захисту інформації	120	4	6			60	30	30		60								4		
ВБ1.5	Захищені мережеві технології обробки інформації	150	5	3			60	30	30		90					4					
ВБ1.6	Безпека при експлуатації і обслуговуванні IT систем	120	4	7			60	30	30		60									4	
ВБ1.7	Крос-платформне програмування	120	4	7			60	30	30		60									4	
ВБ1.8	Безпека розробки і підтримки додатків	120	4	8			48	24	24		72										4
ВБ1.9	Навчальна практика з програмування	180	6									180									
ВБ1.10	Навчальна практика з технологій захисту інформації	180	6									180									
ВБ1.11	Адміністрування комп'ютерних мереж	150	5	8			60	24	36		90										5
ВБ1.12	Управління проектами захисту інформації	120	4	8			48	24	24		72										4
ВБ1.13	Програмування в середовищі сучасних ОС	150	5	8			60	24	36		90										5
Всього		**1800**	**60**	**11**			**621**	**291**	**330**		**819**	**360**				**4**		**11**	**4**	**8**	**18**
Вибірковий блок 2 «Управління інформаційною безпекою»																					

№ п.п.	Дисципліни	Загальний обсяг		Форми контролю знань (за семестрами)			Аудиторні заняття				Самостійна робота	Практична підготовка		Розподіл тижневих годин за курсами та семестрами							
								у тому числі						I курс		II курс		III курс		IV курс	
														Семестри							
														1	2	3	4	5	6	7	8
														Кількість тижнів у семестрі							
		Годин	Кредитів	Іспит	Залік	Курсова робота (проект)	**Всього**	лекції	лабораторні	практичні		Навч. практика	Виробн. практика	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**12**
ВБ2.1	Технології комп'ютерного проектування систем захисту інформації	120	4	5			60	30	30		60							4			
ВБ2.2	Системи прийняття рішень в завданнях захисту інформації	120	4	5			45	15	30		75							3			
ВБ2.3	Сучасні технології програмування	150	5	5			60	30	30		90							4			
ВБ2.4	Безпека безпровідних, мобільних та хмарних технологій	120	4	6			60	30	30		60								4		
ВБ2.5	Основи аудиту інформаційної безпеки	150	5	3			60	30	30		90					4					
ВБ2.6	Архітектура і моделі безпеки	120	4	7			60	30	30		60									4	
ВБ2.7	Програмування на мові Java	120	4	7			60	30	30		60									4	
ВБ2.8	Проведення розслідувань інцидентів інформаційної безпеки	120	4	8			48	24	24		72										4
ВБ2.9	Навчальна практика з комп'ютерних технологій	180	6									180									
ВБ2.10	Навчальна практика з проектування ЦП	180	6									180									
ВБ2.11	Управління веб-контентом	150	5	8			60	24	36		90										5
ВБ2.12	Продукти та послуги інформаційної безпеки	120	4	8			48	24	24		72										4
ВБ2.13	Розробка додатків в сучасних ОС	150	5	8			60	24	36		90										5
Всього		**1800**	**60**	**11**			**621**	**291**	**330**		**819**	**360**				**4**		**11**	**4**	**8**	**18**
Загальний обсяг вибіркових компонентів		**2880**	**96**	**20**	**7**		**1251**	**486**	**390**	**375**	**1389**	**360**		**14**	**8**	**8**	**8**	**15**	**4**	**12**	**18**
Всього годин навчальних занять (без військової підготовки)		**7200**	**240**	**45**	**11**		**3183**	**1377**	**1311**	**495**	**3387**	**750**		**30**	**30**	**28**	**28**	**26**	**27**	**24**	**24**
	Кількість екзаменів				**45**									3	6	5	6	7	6	7	5
	Кількість заліків				**11**										1	2	2		1		
	Кількість курсових проектів і робіт														1	1	1	1	1	1	
	РАЗОМ за ОС	**7200**	**240**																		

ІІІ.СТРУКТУРА НАВЧАЛЬНОГО ПЛАНУ

Навчальні дисципліни	Години	Кредити	%
1. Обов'язкові компоненти ОПП	**4320**	**144**	**60,0**
2Вибіркові компоненти ОПП			
Вибірковий блок 1 (за вибором університету)	**1080**	**36**	**15,0**
Вибірковий блок 2 (за вибором студента)	**1800**	**60**	**25,0**
3. Інші види навчання			
Разом за ОКР	**7200**	**240**	**100,0**

IV. ЗВЕДЕНІ ДАНІ ПРО БЮДЖЕТ ЧАСУ, ТИЖНІ

Рік навчання	Теоретичне навчання	Екзаменаційна сесія	Практична підготовка	Підготовка бакалаврської роботи	Державна 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 ОКР	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	180	6	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	30	1		+	4
4	Основи криптографічного та стеганографічного захисту інформації	30	1	+		5
5	Безпека інформації в інформаційно-комунікаційних системах	15	0,5	+		6
6	Технології захисту інформації	30	1	+		7

VII. ДЕРЖАВНА АТЕСТАЦІЯ

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