(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

ОСВІТНЬО –ПРОФЕСІЙНА ПРОГРАМА

«Системи технічного захисту інформації, автоматизація її обробки»
(найменування ОПП)

Першого (бакалаврського) рівня вищої освіти

за спеціальністю 125 Кібербезпека
(шифр та найменування спеціальності)

галузі знань 12 Інформаційні технології
(шифр та найменування галузі)

освітня кваліфікація: Бакалавр з кібербезпеки
(найменування кваліфікації)

СМЯ НАУ ОПП 14.01.04 – 01 – 2018

Затверджено Вченою радою
Голова Вченої ради
_____ І.Сасенко
(протокол № 5 від 26.06.2018р.)

Освітньо-професійна програма
вводиться в дію наказом ректора
Ректор
_____ В. Ісасенко
(наказ №____від_____2018р.)

КИЇВ

ДІЄ ЯК ТИМЧАСОВА ДО ВВЕДЕННЯ СТАНДАРТУ ВИЩОЇ ОСВІТИ УКРАЇНИ

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

ПОГОДЖЕНО
Науково-методичною радою університету
протокол № 5
від "04" 06 2018 р
Проректор НАУ
(Гуделіанен А.І.

ПОГОДЖЕНО
Вченою радою Навчально-наукового інституту інформаційно-діагностичних систем
протокол № 5
від "22" травня 2018 р
Голова Вченої ради Навчально-наукового інституту інформаційно-діагностичних систем
(Гумен М.Б.)

ПОГОДЖЕНО
Кафедрою засобів захисту інформації
протокол засідання № 5
від "05" березня 2018 р
Завідувач кафедри
(Козловський В. В.)

ПОГОДЖЕНО
Науково-методично-редакційною радою
Навчально-наукового інституту інформаційно-діагностичних систем
протокол № 5
від "15" травня 2018 р
Голова НМР Навчально-наукового інституту інформаційно-діагностичних систем
(Павленко П.М.)

ПЕРЕДМОВА

РОЗРОБЛЕНО РОБОЧОЮ ГРУПОЮ (спеціальності 125 Кібербезпека) у складі:

КЕРІВНИК РОБОЧОЇ ГРУПИ:

КОЗЛОВСЬКИЙ В.В., д.т.н., проф., завідувач кафедри засобів захисту інформації Навчально-наукового інституту інформаційно-діагностичних систем _____
(підпис)

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

ШВЕЦЬ В.А., к.т.н., доцент, доцент кафедри засобів захисту інформації Навчально-наукового інституту інформаційно-діагностичних систем _____
(підпис)

ТЕМНІКОВ В.О., к.т.н., доцент, доцент кафедри засобів захисту інформації Навчально-наукового інституту інформаційно-діагностичних систем _____
(підпис)

НІМЧЕНКО Т.В., к.т.н., доцент, доцент кафедри засобів захисту інформації Навчально-наукового інституту інформаційно-діагностичних систем _____
(підпис)

ЛАЗАРЕНКО С.В., к.т.н., доцент, доцент кафедри засобів захисту інформації Навчально-наукового інституту Інформаційно-діагностичних систем _____
(підпис)

Рецензент Оксіюк О.Г., завідувач кафедри кібербезпеки та захисту інформації Факультету інформаційних технологій Київського національного університету імені Тараса Шевченка, доктор технічних наук, професор.

Рецензії-відгуки зовнішніх стейкхолдерів (додаються).

Рівень документа – 3б
Плановий термін між ревізіями – 1 рік
Контрольний примірник

1. Профіль освітньо-професійної програми

Розділ 1. Загальна інформація		
1.1.	Повна назва закладу вищої освіти та структурного підрозділу	Національний авіаційний університет, Навчально-науковий інститут інформаційно-діагностичних систем Кафедра засобів захисту інформації
1.2.	Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр; Бакалавр з кібербезпеки
1.3.	Офіційна назва освітньо-професійної програми	Освітньо-професійна програма Системи технічного захисту інформації, автоматизація її обробки
1.4.	Тип диплому та обсяг освітньо-професійної програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 4 роки
1.5.	Наявність акредитації	Акредитаційна комісія, Міністерство освіти і науки України, сертифікат серія НД-ІІ № 1181256 від 18.01.2017
1.6.	Цикл/рівень	FQ-EHEA – перший цикл, НРК – 7 рівень
1.7.	Передумови	Повна загальна середня освіта
1.8.	Мова(и) викладання	Українська
1.9.	Термін дії освітньо-професійної програми	-
1.10	Інтернет-адреса постійного розміщення опису освітньо-професійної програми	http://www.nau.edu.ua http://www.iids.nau.edu.ua
Розділ 2. Мета освітньо-професійної програми		
2.1.	Мета освітньої програми полягає в оволодінні студентами знаннями, вміннями та навичками використовувати і впроваджувати технології інформаційної та/або кібербезпеки	
Розділ 3. Характеристика освітньо-професійної програми		
3.1	Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	Галузь знань: 12 Інформаційні технології Спеціальність: 125 Кібербезпека
3.2.	Орієнтація освітньо-професійної програми	Освітньо-професійна, базується на загальновідомих наукових результатах в галузі інформаційних технології у рамках яких можлива подальша професійна кар'єра і подальше навчання.
3.3.	Основний фокус освітньо-професійної програми та спеціалізації	Загальна вища освіта
3.4.	Особливості освітньо-професійної програми	Програма передбачає вивчення: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або

		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 та локалізації каналів витоку інформації; – методів та засобів виявлення закладних пристроїв; – методів та засобів оцінювання захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – автоматизованих систем проектування.
Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1.	Придатність до працевлаштування	Випускники підготовлені до роботи за національним класифікатором України : - фахівець з питань безпеки підприємств, установ та організацій; -фахівець із організації інформаційної безпеки; -фахівець із організації захисту інформації з обмеженим доступом; -фахівець з режиму секретності; - фахівець з досліджень та розробок; - інспектор з організації захисту секретної інформації.
4.2.	Подальше навчання	Продовження навчання за програмою другого рівня вищої освіти (магістр).
Розділ 5. Викладання та оцінювання		
5.1.	Викладання та навчання	Лекції, лабораторні роботи, семінари, практичні заняття, проектна робота в командах, самостійна робота на основі підручників та конспектів, консультації з викладачами, виробнича та переддипломна практика на підприємствах, підготовка дипломній роботи.
5.2.	Оцінювання	Усні та письмові екзамени, лабораторні звіти, курсові роботи, презентації, поточний контроль, захист дипломного проекту.
Розділ 6. Програмні компетентності		
6.1.	Інтегральні Компетентності (ІК)	ІК1. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

6.2.	Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області та розуміння професії. ЗК3. Здатність професійною спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК5. Здатність до пошуку, оброблення та аналізу інформації. ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ЗК7. 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. ЗК8. Здатність до критики й самокритики, креативність, адаптивність і комунікабельність, наполегливість у досягненні мети, толерантність. ЗК9. Здатність використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
6.3.	Фахові компетентності (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 та/або кібербезпеки. ФК3. Здатність до використання програмних, апаратних та програмно-апаратних комплексів засобів захисту інформації на об'єктах інформаційної діяльності.

6.3.	Фахові компетентності (ФК)	ФК4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. ФК5. Здатність оцінювати захищеність інформації усіх видів, що циркулює на об'єктах інформаційної діяльності. ФК6. Здатність відновлювати штатне функціонування комплексів технічного захисту інформації після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. ФК7. Здатність впроваджувати та забезпечувати функціонування комплексів технічного захисту інформації на об'єктах інформаційної діяльності (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). ФК8. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). ФК9. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. ФК10. Здатність застосовувати методи та засоби криптографічного та стеганографічного захисту інформації на об'єктах інформаційної діяльності. ФК11. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному/кібернетичному простору та інформаційним ресурсам. ФК12. Здатність виявляти та блокувати канали витоку інформації, методи несанкціонованого доступу до інформації, джерел і способів дестабілізуючого впливу на інформацію, здійснювати пошук закладних пристроїв. ФК13. Здатність оцінювати та визначати фізичні процеси, які висвітлюють характеристики та параметри напівпровідникових активних елементів, а також проводити лінійний та нелінійний аналіз електричних схем, схемотехніки різноманітних підсилювальних каскадів, операційних підсилювачів та елементів логіки. ФК14. Здатність застосовувати теоретичні знання та практичні навички з визначення загроз інформації в автоматизованих системах.

6.3.	Фахові компетентності (ФК)	ФК15. Здатність застосовувати методи та засоби організаційного напрямку, щодо захисту інформації на об'єктах інформаційної діяльності. ФК16. Здатність використовувати знання та практичні навички по здійсненню технічного обслуговування, контролю й діагностики комплексної системи захисту інформації на об'єктах інформаційної діяльності. ФК17. Здатність використовувати теоретичні знання та практичні навички з підготовки технічної документації.
Розділ 7. Програмні результати навчання		
7.1.	Програмні результати навчання (ПРН)	ПРН1. Здійснювати професійну діяльність на основі законодавчої та нормативно-правової бази держави, а також у відповідності до вітчизняних і міжнародних вимог і стандартів в галузі інформаційної безпеки і \або кібербезпеки; приймати участь у розробці нормативних документів, концепцій, політик, внутрішніх стандартів, положень, інструкцій, рекомендацій, готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки. ПРН2. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних та наукоємних технологій та методів; забезпечувати професійну діяльність на основі знань і навичок про архітектуру інформаційної системи на основі визначення інформаційних суб'єктів та об'єктів інформаційної діяльності, корпоративної архітектури, периметру безпеки (контрольованої зони), політики безпеки, привілеїв. ПРН3. Використовувати методи аналізу й діагностики стану програмних, апаратних та програмно-апаратних засобів і систем захисту інформації; забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. ПРН4. Визначати відомості, які відносяться до інформації з обмеженим доступом, організовувати допуск та доступ персоналу до інформації з обмеженим доступом згідно чинного законодавства та встановленої політики

7.1.	Програмні результати навчання (ПРН)	інформаційної та/або кібербезпеки. ПРН5. Організовувати внутрішньо-об'єктовий та пропускний режими на підприємстві. ПРН6. Організовувати контроль за станом захисту інформації з обмеженим доступом на об'єктах інформаційної діяльності. ПРН7. Забезпечувати систему безперервності бізнес процесів та відновлення штатного функціонування комплексів засобів захисту інформації на основі встановленої процедури планування, вимог, правил безпеки з урахуванням аналізу небезпечних впливів, превентивних мір, стратегій відновлення інфраструктури, резервування різних типів; здійснювати задачі корекції та тестування, перегляду цілей, стратегій, планів після реалізації загроз порушником, здійснення кібератак, збоїв та відмов різних класів, що привело до порушень штатного функціонування комплексів засобів захисту інформації. ПРН8. Вирішувати задачі забезпечення та супроводу комплексу технічного захисту інформації на об'єкті інформаційної діяльності, а також протидії несанкціонованому доступу до інформації згідно встановленої політики інформаційної і\або кібербезпеки. ПРН9. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованим вторгненням до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; ПРН10. Здатність продемонструвати знання та вміння забезпечувати систему виявлення, ідентифікації, аналізу та реагування на інциденти з метою забезпечення захисту інформації від різного класу загроз та кібератак; застосовувати національні та міжнародні регулюючі акти, процедури та положення в сфері інформаційної безпеки та/або кібербезпеки для збору доказів і проведення розслідування інцидентів порушення безпеки інформації. ПРН11. Вирішувати задачі захисту інформації, що обробляється в АС (ІТС) з використанням сучасних методів та засобів криптографічного та стеганографічного захисту інформації. ПРН12. Здатність здійснювати оцінювання

7.1.	Програмні результати навчання (ПРН)	захищеності інформації усіх видів, що циркулює на об'єкті інформаційної діяльності. ПРН13. Здатність забезпечення функціонування системи моніторингу управління доступом до інформації на об'єктах інформаційної діяльності і процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем в умовах реалізації загроз різних класів та протидії порушникам. ПРН14. Здатність застосування систем виявлення та протидії несанкціонованим вторгненням на об'єкти інформаційної діяльності, використання засобів пошуку каналів витоку інформації та закладних пристроїв. ПРН15. Здатність продемонструвати знання та розуміння основ схемотехніки та описати в загальних поняттях і термінах принципи дії, основні характеристики, параметри і особливості застосування електронних напівпровідникових приладів та інтегральних схем, підсилювальних каскадів, операційних підсилювачів та елементів логіки що використовуються в обчислювальній техніці, автоматичних пристроях, комп'ютерних системах та мережах. ПРН16. Здатність продемонструвати знання та розуміння основ побудови комп'ютерних систем захисту інформації та описати в загальних поняттях і термінах архітектуру, характеристики та принципи їх дії. ПРН17. Здатність продемонструвати знання та розуміння основ побудови комп'ютерних мереж та описати в загальних поняттях і термінах принципи та методи організації мережевих комунікацій; архітектуру та функціонування локальних, комбінованих і глобальних комп'ютерних мереж; систему мережевих стандартів, способи адресації та протоколи маршрутизації. ПРН18. Здатність продемонструвати знання та розуміння сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. ПРН19. Здатність продемонструвати знання та розуміння захисту інформації на об'єктах інформаційної діяльності та обґрунтовано обирати і застосовувати на практиці методи виявлення інформаційних загроз; програмні та програмно-апаратні засоби захисту інформації; методи протидії спробам несанкціонованого

7.1.	Програмні результати навчання (ПРН)	доступу до інформаційних ресурсів; організаційні та адміністративні заходи підвищення рівня інформаційної та/або кібербезпеки. ПРН20. Здатність продемонструвати знання та навички складання технічної документації. ПРН21. Оволодіння навичками працювати самостійно при виконанні курсових робіт, курсових проектів, дипломних робіт. ПРН22. Здатність володіння англійською мовою, використовувати спеціальну термінологію для проведення літературного пошуку.
Розділ 8. Ресурсне забезпечення реалізації програми		
8.1.	Кадрове забезпечення	Всі науково-педагогічні працівники, що забезпечують освітньо- професійну програму за кваліфікацією відповідають профілю і напряму дисциплін, що викладаються, мають необхідний стаж педагогічної роботи та досвід практичної роботи. В процесі організації навчального процесу залучаються професіонали з досвідом дослідницької, управлінської, інноваційної, творчої та фахової роботи, іноземні лектори.
8.2.	Матеріально-технічне забезпечення	Навчальні приміщення, комп'ютерні робочі місця, мультимедійні класи дозволяють повністю забезпечити освітній процес протягом усього циклу підготовки за освітньою програмою.
8.3	Інформаційне та навчально-методичне забезпечення	Офіційний веб-сайт www.nau.edu.ua містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти. Матеріали навчально-методичного забезпечення освітньої програми викладені в репозитарії НАУ за посиланням: http://er.nau.edu.ua/handle/NAU/9190 Всі ресурси науково-технічної бібліотеки доступні через сайт університету: http://www.lib.nau.edu.ua Читальний зал забезпечений бездротовим доступом до мережі Інтернет. Електронний репозитарій наукової бібліотеки НАУ: http://er.nau.edu.ua
Розділ 9. Академічна мобільність		
9.1.	Національна кредитна мобільність	Двосторонні договори між Національним авіаційним університетом та Технічним університетом України (КПІ) та Харківським національним університетом радіоелектроніки.

9.2.	Міжнародна кредитна мобільність	У рамках Еразмус+К1 договір про співробітництво між Національним авіаційним університетом та навчальними закладами ЕС.
9.3.	Навчання іноземних здобувачів вищої освіти	Створено умови для навчання іноземних здобувачів вищої освіти.

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

2.1. Перелік компонент ОПП

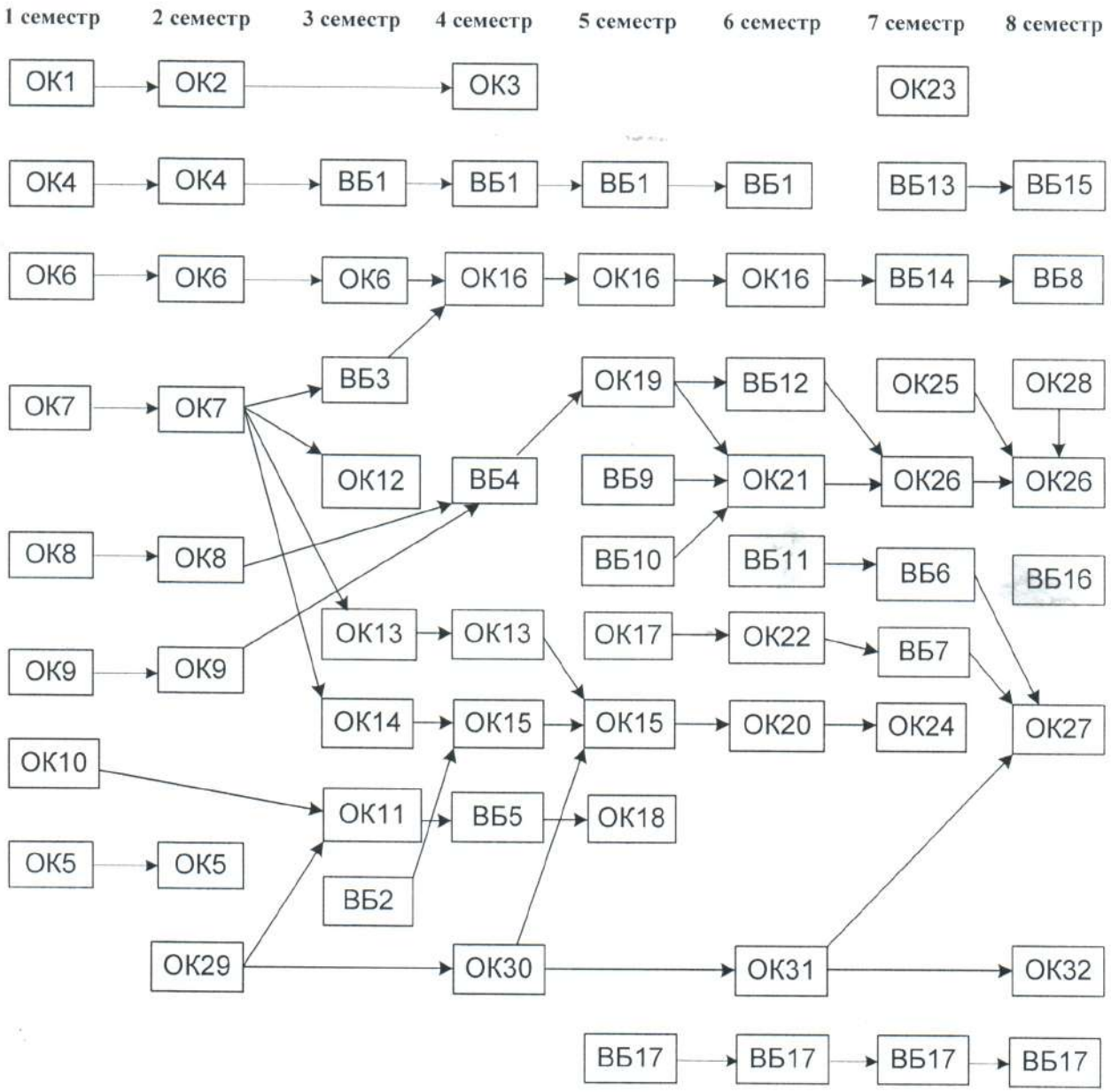
Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОПП			
ОК1.	Українська мова	3.0	Екзамен
ОК2.	Історія та культура України	3.0	Екзамен
ОК3.	Філософія	3.0	Екзамен
ОК4.	Іноземна мова	4.0	Екзамен, Диференційований залік
ОК5.	Фізичне виховання	3.0	Диференційований залік
ОК6.	Вища математика	17	Екзамен, Диференційований залік
ОК7.	Фізика	10.0	Диференційований залік
ОК8.	Інформаційні технології + КР (курсова робота)	12.5	Екзамен
ОК9.	Комп'ютерна графіка	6.0	Екзамен, Диференційований залік
ОК10.	Основи інформаційної безпеки держави	4.0	Екзамен
ОК11.	Основи проектування систем технічного захисту інформації	4.0	Екзамен
ОК12.	Метрологія та вимірювання	3.5	Екзамен
ОК13.	Основи теорії кіл, сигналів та процесів в системах технічного захисту інформації + КР (курсова робота)	10.0	Екзамен
ОК14.	Компонентна база засобів технічного захисту інформації	4.0	Екзамен
ОК15.	Схемотехніка пристроїв технічного захисту інформації + КР (курсова робота)	10.5	Екзамен

1	2	3	4
ОК16.	Поля і хвилі в системах технічного захисту інформації + КР (курсова робота)	14.0	Екзамен
ОК17.	Засоби передавання інформації в системах технічного захисту інформації	4.5	Екзамен
ОК18.	Теорія інформації та кодування	3.5	Диференційований залік
ОК19.	Безпека інформаційно-комунікаційних систем	3.0	Екзамен
ОК20.	Мікропроцесори в системах технічного захисту інформації	4.0	Екзамен
ОК21.	Управління інформаційною безпекою	3.0	Диференційований залік
ОК22.	Засоби приймання та обробки інформації в системах технічного захисту інформації + КП (курсовий проект)	5.0	Екзамен
ОК23.	Основи охорони праці	3.0	Диференційований залік
ОК24.	Цифрова обробка сигналів	4.0	Диференційований залік
ОК25.	Технічні засоби охорони об'єктів + КП (курсовий проект)	5.0	Екзамен
ОК26.	Методи та засоби технічного захисту інформації	7.5	Екзамен
ОК27.	Проектування систем технічного захисту інформації + КР (курсова робота)	5.0	Екзамен
ОК28.	Криптографія та стеганографія	3.0	Диференційований залік
ОК29.	Фахово-ознайомлювальна практика	3.0	Диференційований залік
ОК30.	Схемотехнічна практика	3.0	Диференційований залік
ОК31.	Технологічна практика	4.5	Диференційований залік
ОК32.	Дипломне проектування	7.5	Захист
Загальний обсяг обов'язкових компонент:		180 кредитів	
Вибіркові компоненти ОПП			
ВБ1.	Іноземна мова (за професійним спрямуванням)	8.0	Диференційований залік
ВБ2.	Пристрої електроживлення систем технічного захисту інформації	3.0	Диференційований залік
ВБ3.	Спеціальні розділи фізики	3.0	Диференційований залік
ВБ4.	Комп'ютерні мережі	3.0	Диференційований залік
ВБ5.	Системи запису і відтворення інформації	3.5	Диференційований залік

1	2	3	4
ВБ6.	Організаційне забезпечення технічного захисту інформації	3.5	Диференційований залік
ВБ7.	Системи технічного захисту інформації	3.5	Диференційований залік
ВБ8.	Радіопротидія	3.5	Екзамен
ВБ9.	Економіка інформаційної безпеки*	3.5	Диференційований залік
ВБ10.	Системи банківської безпеки*	3.5	Диференційований залік
ВБ11.	Нормативно-правове забезпечення інформаційної безпеки*	3.0	Диференційований залік
ВБ12.	Комплексні системи захисту інформації*	4.5	Екзамен
ВБ13.	Аналітична обробка даних*	3.5	Диференційований залік
ВБ14.	Електромагнітна сумісність і завадостійкість систем технічного захисту інформації*	3.5	Диференційований залік
ВБ15.	Аудит інформаційної безпеки*	3.0	Екзамен
ВБ16.	Кібербезпека хмарних технологій*	4.5	Диференційований залік
ВБ17.	Військова підготовка	29.0	Екзамен Диференційований залік
Загальний обсяг вибіркових компонент		60 кредитів	
Загальний обсяг освітньо-професійної програми		240 кредитів	

* - дисципліни альтернативні військовій підготовці

2.2. Структурно-логічна схема ОПП



3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньо-професійної програми проводиться у формі захисту дипломної роботи та завершується видачею документу встановленого зразка про присудження йому освітнього ступеня бакалавра із присвоєнням освітньої кваліфікації: Бакалавр з кібербезпеки за спеціальністю 125 Кібербезпека.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ВБ 1	ВБ 2	ВБ 3	ВБ 4	ВБ 5	ВБ 6	ВБ 7	ВБ 8	ВБ 9	ВБ 10	ВБ 11	ВБ 12	ВБ 13	ВБ 14	ВБ 15	ВБ 16
ЗК1	+							+	+		+	+			+		+	+	+	+	+	+	+		+	+	+	+	+	+	+	+				+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК2								+		+	+								+		+					+	+										+							+	+			+	+
ЗК3	+			+																													+						+										
ЗК4										+	+								+		+				+		+		+	+	+							+	+				+	+	+	+	+	+
ЗК5	+			+				+																+	+				+	+	+	+	+											+		+	+
ЗК6	+	+	+																																														
ЗК7	+	+						+		+																																							
ЗК8	+																																																
ЗК9					+																																												
ФК1	+			+						+									+				+								+	+						+				+	+	+			+	+
ФК2								+			+								+		+					+		+										+				+		+			+	+
ФК3											+		+	+	+		+					+							+	+	+			+			+		+								
ФК4								+		+	+								+		+		+		+	+	+										+					+	+				+	
ФК5								+			+	+							+		+	+		+	+	+	+		+	+	+							+	+					+	+			+	+
ФК6														+	+		+			+		+	+		+					+	+			+			+		+	+						+		
ФК7									+		+	+					+					+			+	+	+							+				+	+				+			+		
ФК8								+	+			+							+		+																					+	+					
ФК9																			+		+				+																			+	+		+		+	+
ФК10						+												+	+									+																					
ФК11								+		+									+		+					+				+	+						+		+				+	+	+		+	+
ФК12							+	+			+					+	+						+		+	+	+			+	+					+		+	+	+	+		+			+		
ФК13						+	+	+	+			+	+	+	+	+				+				+						+				+	+											+		
ФК14										+								+	+		+			+		+				+	+					+						+	+	+		+	+
ФК15								+		+	+														+	+	+										+						+				+	
ФК16											+	+							+		+						+			+	+									+					+				+
ФК17	+								+		+										+							+	+	+	+							+					+	+			+	

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

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ВБ 1	ВБ 2	ВБ 3	ВБ 4	ВБ 5	ВБ 6	ВБ 7	ВБ 8	ВБ 9	ВБ 10	ВБ 11	ВБ 12	ВБ 13	ВБ 14	ВБ 15	ВБ 16
ПРН1										+		+											+																	+		+				+	+
ПРН2						+	+	+										+	+																														
ПРН3								+				+						+			+																						+				+	
ПРН4										+	+										+																	+					+				+	
ПРН5								+			+										+				+	+											+	+				+		+				
ПРН6										+	+								+		+						+										+	+				+	+					
ПРН7											+								+		+		+			+																		+		+		
ПРН8											+														+	+	+							+			+	+										
ПРН9								+	+										+		+															+						+	+	+				+
ПРН10											+								+		+																						+	+	+			+	+
ПРН11						+	+	+										+						+				+															+						
ПРН12								+		+	+	+							+		+					+	+															+	+		+			
ПРН13								+		+	+							+	+		+					+											+						+	+		+			
ПРН14						+	+				+				+		+			+		+		+		+	+															+	+					
ПРН15							+						+	+	+	+				+														+												+			
ПРН16								+	+										+																		+												
ПРН17						+		+	+										+																		+												
ПРН18										+	+								+		+					+																	+				+	+
ПРН19											+				+										+	+	+												+	+								
ПРН20									+		+				+												+												+					+				
ПРН21	+							+	+		+												+		+	+	+					+						+	+				+				
ПРН22				+				+																																			+					

(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки
1		09.07.18	Мельниченко В.А.		

(Ф 03.02 – 02)

АРКУШ ОЗНАЙОМЛЕННЯ З ДОКУМЕНТОМ

№ пор.	Прізвище ім'я по-батькові	Підпис ознайомленої особи	Дата ознайом-лення	Примітки

(Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

№ пор.	Прізвище ім'я по-батькові	Дата ревізії	Підпис	Висновок щодо адекватності

(Ф 03.02 – 03)

АРКУШ ОБЛІКУ ЗМІН

№ зміни	№ листа (сторінки)				Підпис особи, яка внесла зміну	Дата внесення зміни	Дата введення зміни
	Зміненого	Заміненого	Нового	Анульо-ваного			

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				
Узгоджено				