Додатки до освітньо-професійної програми
«Кіберзахист у сфері інформаційних технологій та кіберпросторі»

Додаток 1

Каталог освітнього компонента

№ з/п	Назва складової каталогу	Зміст
1.	Галузь знань	К Безпека та оборона
1.1.	Спеціальність	К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
1.2.	Рівень вищої освіти	Другий (магістерський)
2.	Назва навчальної дисципліни	**ОК-1. Методологія наукових досліджень та академічна доброчесність**
3.	Тип навчальної дисципліни (спецкурсу) (обов'язкова або вибіркова, спеціалізація)	Обов'язкова
4.	Курс (семестр), у якому вивчається	1 (1)
5.	Необхідні обов'язкові попередні та супутні навчальні дисципліни (спецкурси), у тому числі розділи, теми таких дисциплін, спецкурсів, модулів	Компетентності та здатності продемонструвати результати навчання, визначені стандартом вищої освіти за спеціальністю 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) для першого (бакалаврського) рівня вищої освіти.
6.	Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах	**3 ЄКТС/ 90 год.**, зокрема для: - лекційних занять – 12 год. / 6 год. (заочна); - семінарських занять – 10 год. / 4 год. (заочна); - практичних (лабораторних) занять – 10 год. / 2 год. (заочна); - самостійної роботи – 58 год. / 78 год (заочна).
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 5. Розробляти та реалізовувати інноваційні проєкти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів. ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН 11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання професійних задач у визначених законодавством сферах та за напрямами майбутньої діяльності. ПРН 14. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців,

		зокрема до осіб, які навчаються. ПРН 17. Створювати та документально оформлювати організаційно-технічні та організаційно-правові моделі кіберзахисту, а також моделі захисту конфіденційності, організовувати та розробляти системи кіберзахисту у сфері інформаційних технологій та кіберпростору, здійснювати моніторинг та аудит інформаційної безпеки та кібербезпеки на підприємствах, установах та організаціях різних форм власності.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Змістовний модуль 1. Основи організації та методологія наукових досліджень. Тема 1. Наука та наукові дослідження у сучасному світі Тема 2. Методологія наукових досліджень та її значення у науковій роботі. Змістовний модуль 2. Теорія та практика наукових досліджень. Тема 1. Основи когнітивної творчості дослідника Тема 2. Представлення наукових досліджень
9.	Запланована навчальна діяльність та методи навчання	Навчальна діяльність здійснюється шляхом лекційних, семінарських, практичних занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій.
10.	Методи і критерії оцінювання	Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, диференційований залік. Рівень підготовки студентів оцінюється наступним чином: “*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок; “*Дуже добре*” (B) – вище середнього рівня з кількома помилками; “*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок; “*Задовільно*” (D) – непогано, але зі значною кількістю недоліків; “*Достатньо*” (E) – виконання задовольняє мінімальні критерії; “*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку; “*Незадовільно*” (F) – необхідна серйозна подальша робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра філософії
Навчально-наукового гуманітарного інституту

Додаток 2

Каталог освітнього компонента

№ з/п	Назва складової каталогу	Зміст
1.	Галузь знань	К Безпека та оборона
1.1.	Спеціальність	К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
1.2.	Рівень вищої освіти	Другий (магістерський)
2.	Назва навчальної дисципліни	**ОК-2. Риторика та стилістика наукових праць**
3.	Тип навчальної дисципліни (спецкурсу) (обов'язкова або вибіркова, спеціалізація)	Обов'язкова
4.	Курс (семестр), у якому вивчається	1 (1)
5.	Необхідні обов'язкові попередні та супутні навчальні дисципліни (спецкурси), у тому числі розділи, теми таких дисциплін, спецкурсів, модулів	Компетентності та здатності продемонструвати результати навчання, визначені стандартом вищої освіти за спеціальністю 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) для першого (бакалаврського) рівня вищої освіти.
6.	Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах	**3 ЄКТС/ 90 год.**, зокрема для: - лекційних занять – 12 год. / 6 год. (заочна); - семінарських занять – 20 год. / 6 год. (заочна); - самостійної роботи – 58 год. / 78 год (заочна).
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 6. Вільно спілкуватися державною та іноземною мовами усно і письмово для обговорення професійної діяльності, результатів досліджень та інновацій, пошуку та аналізу відповідної інформації. ПРН 14. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Модуль І. Державна мова в науковій комунікації професіонала з організації інформаційної безпеки 1. Специфіка наукового тексту й професійного наукового викладу думки 2. Морфологічні норми фахового наукового мовлення професіонала з організації інформаційної безпеки 3. Синтаксичні норми фахового наукового

		мовлення професіонала з організації інформаційної безпеки 4. Укладання фахового публічного виступу професіонала з організації інформаційної безпеки 5. Мистецтво виголошення фахового публічного виступу професіонала з організації інформаційної безпеки. Мовна поведінка оратора. 6. Культура писемного наукового мовлення професіонала з організації інформаційної безпеки
9.	Запланована навчальна діяльність та методи навчання	Навчальна діяльність здійснюється шляхом лекційних, семінарських занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій.
10.	Методи і критерії оцінювання	Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, диференційований залік. Рівень підготовки студентів оцінюється наступним чином: “*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок; “*Дуже добре*” (B) – вище середнього рівня з кількома помилками; “*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок; “*Задовільно*” (D) – непогано, але зі значною кількістю недоліків; “*Достатньо*” (E) – виконання задовольняє мінімальні критерії; “*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку; “*Незадовільно*” (F) – необхідна серйозна подальша робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра української ділової мови
Навчально-наукового гуманітарного інституту

Додаток 3

Каталог освітнього компонента

№ з/п	Назва складової каталогу	Зміст
1.	Галузь знань	К Безпека та оборона
1.1.	Спеціальність	К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
1.2.	Рівень вищої освіти	Другий (магістерський)
2.	Назва навчальної дисципліни	**ОК-3. Теорія прийняття рішень і управління**
3.	Тип навчальної дисципліни (спецкурсу) (обов'язкова або вибіркова, спеціалізація)	Обов'язкова
4.	Курс (семестр), у якому вивчається	1 (1)
5.	Необхідні обов'язкові попередні та супутні навчальні дисципліни (спецкурси), у тому числі розділи, теми таких дисциплін, спецкурсів, модулів	Компетентності та здатності продемонструвати результати навчання, визначені стандартом вищої освіти за спеціальністю 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) для першого (бакалаврського) рівня вищої освіти.
6.	Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах	**3 ЄКТС/ 120 год.**, зокрема для: - лекційних занять – 12 год. / 6 год. (заочна); - практичних (лабораторних) занять – 20 год. / 6 год. (заочна); - самостійної роботи – 58 год. / 78 год (заочна).
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (кіберзахист, забезпечення державної безпеки в інформаційній сфері), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог. ПРН 4. Організовувати роботу колективу, забезпечувати професійний розвиток його членів та досягнення поставлених цілей. ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН 11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання професійних задач у визначених законодавством сферах та за напрямами майбутньої діяльності. ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах

		обстановки з використанням нових стратегічних підходів. ПРН 16. Організовувати та спрямовувати діяльність фахівців з кіберзахисту у сфері інформаційних технологій та кіберпросторі; розробляти та впроваджувати заходи із кіберзахисту у сфері інформаційних технологій та кіберпросторі, самостійно та у взаємодії з контролюючими органами. ПРН 18. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Змістовний модуль 1. Системне мислення та основи управлінських рішень Тема 1. Системне мислення як інструмент аналізу складних явищ Змістовний модуль 2. Стратегічне мислення та управління майбутнім Тема 1. Розвиток здатності працювати з масштабними системами та їх управлінням Змістовний модуль 3. Проєктування моделей та практика управління Тема 1. Розвиток здатності працювати з масштабними системами та їх управлінням
9.	Запланована навчальна діяльність та методи навчання	Навчальна діяльність здійснюється шляхом лекційних, практичних занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій.
10.	Методи і критерії оцінювання	Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, диференційований залік. Рівень підготовки студентів оцінюється наступним чином: “*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок; “*Дуже добре*” (B) – вище середнього рівня з кількома помилками; “*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок; “*Задовільно*” (D) – непогано, але зі значною кількістю недоліків; “*Достатньо*” (E) – виконання задовольняє мінімальні критерії; “*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;

		“*Незадовільно*” (F) – необхідна серйозна подальша робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра управління та інформаційно-аналітичного забезпечення оперативно-службової діяльності центру стратегічних комунікацій
Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій

Додаток 4

Каталог освітнього компонента

№ з/п	Назва складової каталогу	Зміст
1.	Галузь знань	К Безпека та оборона
1.1.	Спеціальність	К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
1.2.	Рівень вищої освіти	Другий (магістерський)
2.	Назва навчальної дисципліни	**ОК-4. Іноземна мова професійного спрямування**
3.	Тип навчальної дисципліни (спецкурсу) (обов'язкова або вибіркова, спеціалізація)	Обов'язкова
4.	Курс (семестр), у якому вивчається	1 (1), 1(2)
5.	Необхідні обов'язкові попередні та супутні навчальні дисципліни (спецкурси), у тому числі розділи, теми таких дисциплін, спецкурсів, модулів	Компетентності та здатності продемонструвати результати навчання, визначені стандартом вищої освіти за спеціальністю 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) для першого (бакалаврського) рівня вищої освіти.
6.	Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах	**6 ЄКТС / 180 год.**, зокрема для: - практичних (лабораторних) занять – 88 год. / 24 год (заочна); - самостійної роботи – 92 год. / 156 год (заочна).
7.	Програмні результати навчання	ПРН 5. Розробляти та реалізовувати інноваційні проєкти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів. ПРН 6. Вільно спілкуватися державною та іноземною мовами усно і письмово для обговорення професійної діяльності, результатів досліджень та інновацій, пошуку та аналізу відповідної інформації. ПРН 14. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Модуль І. Робота з джерелами інформації. Тема 1. Типи інформаційних джерел. Тема 2. Аналіз наукової літератури професійного спрямування. Тема 3. Типи інформації. Основні характеристики. Модуль ІІ. Інформаційна безпека. Тема 1. Основні засади інформаційної безпеки. Тема 2. Основні загрози інформаційній безпеці.

		Тема 3. Захист інформації, методи і способи протидії основним загрозам. Модуль ІІІ. Стратегії успішного працевлаштуванні. Тема 1. Підготовка необхідних форм документації для успішного працевлаштування. Тема 2. Співбесіда як вирішальний етап працевлаштування.
9.	Запланована навчальна діяльність та методи навчання	Навчальна діяльність здійснюється шляхом практичних занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій.
10.	Методи і критерії оцінювання	Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, диференційований залік та екзамен. Рівень підготовки студентів оцінюється наступним чином: “*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок; “*Дуже добре*” (B) – вище середнього рівня з кількома помилками; “*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок; “*Задовільно*” (D) – непогано, але зі значною кількістю недоліків; “*Достатньо*” (E) – виконання задовольняє мінімальні критерії; “*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку; “*Незадовільно*” (F) – необхідна серйозна подальша робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра романо-германських мов
Навчально-науковий гуманітарний інститут

Додаток 5

Каталог освітнього компонента

№ з/п	Назва складової каталогу	Зміст
1.	Галузь знань	К Безпека та оборона
1.1.	Спеціальність	К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
1.2.	Рівень вищої освіти	Другий (магістерський)
2.	Назва навчальної дисципліни	**ОК-5. Гендерна політика в секторі безпеки та оборони України**
3.	Тип навчальної дисципліни (спецкурсу) (обов'язкова або вибіркова, спеціалізація)	Обов'язкова
4.	Курс (семестр), у якому вивчається	2 (4)
5.	Необхідні обов'язкові попередні та супутні навчальні дисципліни (спецкурси), у тому числі розділи, теми таких дисциплін, спецкурсів, модулів	«Інформаційне протиборство», «Іноземна мова професійного спрямування», «Актуальні проблеми інформаційної безпеки», «Аудит інформаційної безпеки та кібербезпеки»
6.	Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах	**3 ЄКТС/90 год.**, зокрема для: - лекційних занять – 10 год. / 6 год (заочна); - семінарських занять – 20 год. / 6 год (заочна); - самостійної роботи – 60 год. / 78 год (заочна)
7.	Програмні результати навчання	ПРН 4. Організовувати роботу колективу, забезпечувати професійний розвиток його членів та досягнення поставлених цілей. ПРН 8. Забезпечувати дотримання принципу гендерної рівності під час здійснення професійної діяльності. ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Модуль І. Теоретично-правові та практичні питання забезпечення гендерної рівності в секторі безпеки і оборони. Тема 1. Поняття гендер, гендерна рівність, гендерна чутливість у суспільно-політичному та науковому дискурсах. Міжнародно-правове забезпечення гендерної рівності. Українське законодавство щодо гендерних питань Тема 2. Гендерно чутливі комунікації в секторі безпеки і оборони. Передумова, наслідки і протидія дискримінації за ознакою статі. Модуль ІІ. Урахування гендерних підходів у діяльності з питань запобігання шкоди цивільному

		населенню в умовах бойових дій. Тема 1. Гендерний компонент інформаційно-психологічних заходів. Тема 2. Збирання первинних доказів сексуального насильства в умовах війни
9.	Запланована навчальна діяльність та методи навчання	Навчальна діяльність здійснюється шляхом лекційних, семінарських занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій.
10.	Методи і критерії оцінювання	Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, диференційований залік. Рівень підготовки студентів оцінюється наступним чином: “*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок; “*Дуже добре*” (B) – вище середнього рівня з кількома помилками; “*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок; “*Задовільно*” (D) – непогано, але зі значною кількістю недоліків; “*Достатньо*” (E) – виконання задовольняє мінімальні критерії; “*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку; “*Незадовільно*” (F) – необхідна серйозна подальша робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра стратегічних комунікацій та прикладної лінгвістики центру стратегічних комунікацій
Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій

Додаток 6

Каталог освітнього компонента

№ з/п	Назва складової каталогу	Зміст
1.	Галузь знань	К Безпека та оборона
1.1.	Спеціальність	К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
1.2.	Рівень вищої освіти	Другий (магістерський)
2.	Назва навчальної дисципліни	**ОК-6. Розвідка з відкритих джерел інформації (OSINT)**
3.	Тип навчальної дисципліни (спецкурсу) (обов'язкова або вибіркова, спеціалізація)	Обов'язкова
4.	Курс (семестр), у якому вивчається	1 (2)
5.	Необхідні обов'язкові попередні та супутні навчальні дисципліни (спецкурси), у тому числі розділи, теми таких дисциплін, спецкурсів, модулів	Компетентності та здатності продемонструвати результати навчання, визначені стандартом вищої освіти за спеціальністю 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) для першого (бакалаврського) рівня вищої освіти.
6.	Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах	**4 ЄКТС/ 120 год.**, зокрема для: - лекційних занять – 22 год. / 6 год (заочна); - практичних (лабораторних) занять – 22 год. / 8 год. (заочна); - самостійної роботи – 76 год. / 106 год (заочна)
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН 10. Формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності) (кіберзахист, забезпечення державної безпеки в інформаційній сфері). ПРН 16. Організовувати та спрямовувати діяльність фахівців з кіберзахисту у сфері інформаційних технологій та кіберпросторі; розробляти та впроваджувати заходи із кіберзахисту у сфері інформаційних технологій та кіберпросторі, самостійно та у взаємодії з контролюючими органами. ПРН 17. Створювати та документально оформлювати організаційно-технічні та організаційно-правові моделі кіберзахисту, а також

		моделі захисту конфіденційності, організовувати та розробляти системи кіберзахисту у сфері інформаційних технологій та кіберпростору, здійснювати моніторинг та аудит інформаційної безпеки та кібербезпеки на підприємствах, установах та організаціях різних форм власності. ПРН 25. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Модуль І. Інструменти та методи збору інформації Тема 1.1. Поняття та еволюція OSINT. Законодавчі та етичні аспекти використання OSINT Тема 1.2. Класифікація відкрити джерел Тема 1.3. Інструменти збору даних з соціальних мереж (Maltego, SpiderFoot, Social-Searcher), web-пошук Модуль ІІ. OSINT у кібербезпеці Тема 2.1. OSINT для виявлення фішингових кампаній та шкідливих доменів Тема 2.2. Ідентифікація та атрибуція кіберзагроз через OSINT Тема 2.3. Профілювання зловмисників (threat actor profiling) за допомогою відкритих джерел Тема 2.4. Візуалізація OSINT-даних: графи, діаграми, зв'язки
9.	Запланована навчальна діяльність та методи навчання	Навчальна діяльність здійснюється шляхом лекційних, практичних занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій.
10.	Методи і критерії оцінювання	Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, екзамен. Рівень підготовки студентів оцінюється наступним чином: “*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок; “*Дуже добре*” (B) – вище середнього рівня з кількома помилками; “*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок; “*Задовільно*” (D) – непогано, але зі значною кількістю недоліків; “*Достатньо*” (E) – виконання задовольняє мінімальні критерії; “*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку; “*Незадовільно*” (F) – необхідна серйозна подальша

		робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра управління та інформаційно-аналітичного забезпечення оперативно-службової діяльності центру стратегічних комунікацій
Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій

Додаток 7

Каталог освітнього компонента

№ з/п	Назва складової каталогу	Зміст
1.	Галузь знань	К Безпека та оборона
1.1.	Спеціальність	К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
1.2.	Рівень вищої освіти	Другий (магістерський)
2.	Назва навчальної дисципліни	**ОК-7. Інформаційне протиборство**
3.	Тип навчальної дисципліни (спецкурсу) (обов'язкова або вибіркова, спеціалізація)	Обов'язкова
4.	Курс (семестр), у якому вивчається	1(1) денна, 1(2) заочна
5.	Необхідні обов'язкові попередні та супутні навчальні дисципліни (спецкурси), у тому числі розділи, теми таких дисциплін, спецкурсів, модулів	Компетентності та здатності продемонструвати результати навчання, визначені стандартом вищої освіти за спеціальністю 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) для першого (бакалаврського) рівня вищої освіти.
6.	Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах	**5 ЄКТС/ 150 год.**, зокрема для: - лекційних занять – 22 год. / 8 год. (заочне); - семінарських занять – 32 год. / 8 год. (заочне); - самостійної роботи – 96 год. / 134 год. (заочне)
7.	Програмні результати навчання	ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності. ПРН 3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (кіберзахист, забезпечення державної безпеки в інформаційній сфері), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог. ПРН 5. Розробляти та реалізовувати інноваційні проєкти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів. ПРН 8. Забезпечувати дотримання принципу гендерної рівності під час здійснення професійної діяльності. ПРН 11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання професійних задач у визначених законодавством сферах та за напрямами майбутньої діяльності. ПРН 13. Організовувати та здійснювати

		керівництво територіальною обороною, мобілізаційною підготовкою та мобілізацією у межах професійної компетентності. ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів. ПРН 16. Організовувати та спрямовувати діяльність фахівців з кіберзахисту у сфері інформаційних технологій та кіберпросторі; розробляти та впроваджувати заходи із кіберзахисту у сфері інформаційних технологій та кіберпросторі, самостійно та у взаємодії з контролюючими органами. ПРН 20. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН 24. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Змістовий модуль І. Інформаційне протиборство як механізм забезпечення національної безпеки в інформаційній сфері Тема 1. Генезис інформаційного протиборства Тема 2. Сучасні стратегії та концепції інформаційного протиборства Змістовий модуль ІІ. Теоретичні та технологічні основи інформаційного протиборства Тема 3. Теоретичні основи інформаційного протиборства Тема 4. Технології та засоби інформаційного протиборства Змістовий модуль ІІІ. Організаційні аспекти підготовки та ведення інформаційного протиборства Тема 5. Форми ведення інформаційного протиборства Тема 6. Підготовка та ведення інформаційного протиборства з використанням соціально-орієнтованих ресурсів мережі Internet та відкритих даних Тема 7. Перспективи ведення інформаційного протиборства
	Запланована навчальна діяльність та методи	Навчальна діяльність здійснюється шляхом лекційних, семінарських занять та самостійної

	навчання	підготовки з використанням технічних засобів та інформаційних технологій.
10.	Методи і критерії оцінювання	Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, екзамен. Рівень підготовки студентів оцінюється наступним чином: “*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок; “*Дуже добре*” (B) – вище середнього рівня з кількома помилками; “*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок; “*Задовільно*” (D) – непогано, але зі значною кількістю недоліків; “*Достатньо*” (E) – виконання задовольняє мінімальні критерії; “*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку; “*Незадовільно*” (F) – необхідна серйозна подальша робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра інформаційної безпеки держави
Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій

Додаток 8

Каталог освітнього компонента

№ з/п	Назва складової каталогу	Зміст
1.	Галузь знань	К Безпека та оборона
1.1.	Спеціальність	К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
1.2.	Рівень вищої освіти	Другий (магістерський)
2.	Назва навчальної дисципліни	**ОК-8. Прикладні системи штучного інтелекту в кіберпросторі**
3.	Тип навчальної дисципліни (спецкурсу) (обов'язкова або вибіркова, спеціалізація)	Обов'язкова
4.	Курс (семестр), у якому вивчається	1(1)
5.	Необхідні обов'язкові попередні та супутні навчальні дисципліни (спецкурси), у тому числі розділи, теми таких дисциплін, спецкурсів, модулів	Компетентності та здатності продемонструвати результати навчання, визначені стандартом вищої освіти за спеціальністю 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) для першого (бакалаврського) рівня вищої освіти.
6.	Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах	**4 ЄКТС/ 120 год.**, зокрема для: - лекційних занять – 22 год. / 6 год. (заочна); - практичних (лабораторних) занять – 22 год. / 8 год. (заочна); - самостійної роботи – 76 год. / 106 год. (заочна)
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 10. Формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності) (кіберзахист, забезпечення державної безпеки в інформаційній сфері). ПРН 12. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки і є основою для прийняття ефективних рішень, проведення досліджень та критичного осмислення проблем у галузі національної безпеки. ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів. ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення

		ПРН 20. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН 26. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Модуль І. Прикладні системи штучного інтелекту Тема 1.1. Штучний інтелект. Області застосування. Прикладні системи штучного інтелекту Тема 1.2. Інформаційний пошук. Етапи роботи систем інтелектуального аналізу даних. Концепція Data Mining Тема 1.3. Моделі представлення знань. Тема 1.4 Алгоритми пошуку Тема 1.5. Вступ до великих мовних моделей LLM. Ключові компоненти великих мовних моделей. Тема 1.6. Основи роботи з ChatGpt та Perplexity: моделі, режими, функції. Правила побудови промптів. Тема 1.7. Генерування зображень, аудіо та відео файлів з використанням технологій штучного інтелекту.
	Запланована навчальна діяльність та методи навчання	Навчальна діяльність здійснюється шляхом лекційних, практичних занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій.
10.	Методи і критерії оцінювання	Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, екзамен. Рівень підготовки студентів оцінюється наступним чином: "*Відмінно*" (A) – відмінне виконання лише з незначною кількістю помилок; "*Дуже добре*" (B) – вище середнього рівня з кількома помилками; "*Добре*" (C) – у загальному правильна робота з певною кількістю грубих помилок; "*Задовільно*" (D) – непогано, але зі значною кількістю недоліків; "*Достатньо*" (E) – виконання задовольняє мінімальні критерії; "*Незадовільно*" (FX) – потрібно працювати перед тим, як отримати позитивну оцінку; "*Незадовільно*" (F) – необхідна серйозна подальша робота.
11.	Мова навчання	Українська

	(українська та/або іноземні мови)	
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра кібербезпеки центру кібербезпеки
Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій

Додаток 9

Каталог освітнього компонента

№ з/п	Назва складової каталогу	Зміст
1.	Галузь знань	К Безпека та оборона
1.1.	Спеціальність	К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
1.3.	Рівень вищої освіти	Другий (магістерський)
2.	Назва навчальної дисципліни	**ОК-9. Організаційно-правове забезпечення кіберзахисту**
3.	Тип навчальної дисципліни (спецкурсу) (обов'язкова або вибіркова, спеціалізація)	Обов'язкова
4.	Курс (семестр), у якому вивчається	1(1)
5.	Необхідні обов'язкові попередні та супутні навчальні дисципліни (спецкурси), у тому числі розділи, теми таких дисциплін, спецкурсів, модулів	Компетентності та здатності продемонструвати результати навчання, визначені стандартом вищої освіти за спеціальністю 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) для першого (бакалаврського) рівня вищої освіти.
6.	Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах	**5 ЄКТС/ 150 год.**, зокрема для: - лекційних занять – 22 год. / 8 год. (заочна); - семінарських занять – 32 год. / 8 год. (заочна); - самостійної роботи – 96 год. / 134 год (заочна)
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності. ПРН 5. Розробляти та реалізовувати інноваційні проєкти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів. ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН 9. Синтезувати спектр заходів та підходів, що можуть використовуватись для вирішення проблем, пов'язаних з викликами глобальній, європейській та регіональній безпеці. ПРН 10. Формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності) (кіберзахист, забезпечення державної безпеки в інформаційній

		сфері). ПРН 11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання професійних задач у визначених законодавством сферах та за напрямами майбутньої діяльності. ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів. ПРН 17. Створювати та документально оформлювати організаційно-технічні та організаційно-правові моделі кіберзахисту, а також моделі захисту конфіденційності, організовувати та розробляти системи кіберзахисту у сфері інформаційних технологій та кіберпростору, здійснювати моніторинг та аудит інформаційної безпеки та кібербезпеки на підприємствах, установах та організаціях різних форм власності. ПРН 20. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН 25. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. ПРН 26. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Модуль І. Інтереси держави в інформаційній сфері Тема 1.1. Інформаційна складова національної безпеки України Тема 1.2. Політико-правові аспекти формування інформаційного суспільства держави Модуль ІІ. Організаційно-правові засади забезпечення інформаційної безпеки України Тема 2.1. Поняття та види загроз безпеці держави в інформаційній сфері Тема 2.2. Система суб'єктів забезпечення інформаційної безпеки України Тема 2.3. Нормативно-правове забезпечення інформаційної безпеки України
	Запланована навчальна діяльність та методи навчання	Навчальна діяльність здійснюється шляхом лекційних, семінарських занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій.

10.	Методи і критерії оцінювання	Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, екзамен. Рівень підготовки студентів оцінюється наступним чином: “*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок; “*Дуже добре*” (B) – вище середнього рівня з кількома помилками; “*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок; “*Задовільно*” (D) – непогано, але зі значною кількістю недоліків; “*Достатньо*” (E) – виконання задовольняє мінімальні критерії; “*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку; “*Незадовільно*” (F) – необхідна серйозна подальша робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра кібербезпеки центру кібербезпеки
Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій

Додаток 10

Каталог освітнього компонента

№ з/п	Назва складової каталогу	Зміст
1.	Галузь знань	К Безпека та оборона
1.1.	Спеціальність	К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
1.3.	Рівень вищої освіти	Другий (магістерський)
2.	Назва навчальної дисципліни	**ОК-10. Актуальні проблеми інформаційної безпеки**
3.	Тип навчальної дисципліни (спецкурсу) (обов'язкова або вибіркова, спеціалізація)	Обов'язкова
4.	Курс (семестр), у якому вивчається	1 (2)
5.	Необхідні обов'язкові попередні та супутні навчальні дисципліни (спецкурси), у тому числі розділи, теми таких дисциплін, спецкурсів, модулів	«Методологія наукових досліджень та академічна доброчесність», «Теорія прийняття рішень і управління», «Організаційно-правове забезпечення кіберзахисту», «Інформаційне протиборство»
6.	Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах	**5 ЄКТС/ 150 год.**, зокрема для: - лекційних занять – 18 год. / 8 год. (заочна); - семінарських занять – 38 год. / 8 год. (заочна); - самостійної роботи – 94 год. / 134 год. (заочна)
7.	Програмні результати навчання	ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності. ПРН 3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (кіберзахист, забезпечення державної безпеки в інформаційній сфері), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог. ПРН 5. Розробляти та реалізовувати інноваційні проєкти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів. ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН 14. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються. ПРН 16. Організовувати та спрямовувати

		діяльність фахівців з кіберзахисту у сфері інформаційних технологій та кіберпросторі; розробляти та впроваджувати заходи із кіберзахисту у сфері інформаційних технологій та кіберпросторі, самостійно та у взаємодії з контролюючими органами. ПРН 20. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН 23. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Модуль І. Теоретико-правові засади національної безпеки. Тема 1. Основи теорії національної безпеки. Структура національної безпеки. Тема 3. Система суб'єктів забезпечення національної безпеки України. Тема 4. Загрози і виклики національній безпеці. Національні цінності та інтереси Модуль ІІ. Україна в сучасному світі. Тема 1. Глобалізація: нові виклики національній безпеці. Тема 2. Геополітика і політична географія сучасного світу. Тема 3. Місце України в сучасному світі. Тема 4. Доктрини національної безпеки провідних країн світу та сусідніх держав, їх вплив на забезпечення національної безпеки України. Модуль ІІІ. Основні складові національної безпеки. Тема 1. Політична безпека України. Тема 2. Державна безпека України. Тема 3. Економічна та науково-технологічна безпека України. Тема 4. Інформаційна безпека України. Тема 5. Воєнна безпека України. Безпека державного кордону. Тема 6. Соціально-гуманітарна безпека України. Модуль ІV. Служба безпеки України як суб'єкт забезпечення національної безпеки в сфері державної безпеки. Тема 1. Організаційно-правові засади протидії Службою безпеки України основним реальним та потенційним загрозам і викликам національній безпеці та національним інтересам України у сучасних умовах.

9.	Запланована навчальна діяльність та методи навчання	Навчальна діяльність здійснюється шляхом лекційних, семінарських занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій.
10.	Методи і критерії оцінювання	Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, екзамен. Рівень підготовки студентів оцінюється наступним чином: “*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок; “*Дуже добре*” (B) – вище середнього рівня з кількома помилками; “*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок; “*Задовільно*” (D) – непогано, але зі значною кількістю недоліків; “*Достатньо*” (E) – виконання задовольняє мінімальні критерії; “*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку; “*Незадовільно*” (F) – необхідна серйозна подальша робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра інформаційної безпеки держави
Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій

Додаток 11

Каталог освітнього компонента

№ з/п	Назва складової каталогу	Зміст
1.	Галузь знань	К Безпека та оборона
1.1.	Спеціальність	К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
1.2.	Рівень вищої освіти	Другий (магістерський)
2.	Назва навчальної дисципліни	**ОК-11. Системне адміністрування та організація безпеки ІТ-сервісів**
3.	Тип навчальної дисципліни (спецкурсу) (обов'язкова або вибіркова, спеціалізація)	Обов'язкова
4.	Курс (семестр), у якому вивчається	1 (2)
5.	Необхідні обов'язкові попередні та супутні навчальні дисципліни (спецкурси), у тому числі розділи, теми таких дисциплін, спецкурсів, модулів	Компетентності та здатності продемонструвати результати навчання, визначені стандартом вищої освіти за спеціальністю 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) для першого (бакалаврського) рівня вищої освіти.
6.	Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах	**5 ЄКТС/ 150 год.**, зокрема для: - лекційних занять – 18 год. / 8 год (заочна); - практичних (лабораторних) занять – 38 год. / 8 год. (заочна); - самостійної роботи – 94 год. / 134 год (заочна)
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (кіберзахист, забезпечення державної безпеки в інформаційній сфері), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог. ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН 16. Організовувати та спрямовувати діяльність фахівців з кіберзахисту у сфері інформаційних технологій та кіберпросторі; розробляти та впроваджувати заходи із кіберзахисту у сфері інформаційних технологій та кіберпросторі, самостійно та у взаємодії з контролюючими органами. ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту,

		технології створення та використання спеціалізованого програмного забезпечення ПРН 23. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ПРН 26. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Модуль І. Основи системного адміністрування Тема 1.1.Типи серверів . Інсталяція та конфігурація операційних систем на серверному обладнанні Тема 1.2. Налаштування мережевих служб DHCP, DNS, NAT, VPN Тема 1.3. Адміністрування домену Active Directory, LDAP Тема 1.4. Автоматизація процесів та написання скриптів Модуль ІІ. Адміністрування поштових систем Тема 2.1. Розгортання та конфігурація Microsoft Exchange Server. Тема 2.2. Поштові скриньки, налаштування антиспаму, використання SPF, DKIM, DMARC Тема 2.3. Система електронного адміністрування як один із основних ІТ-сервісів Тема 2.3. Організація безпеки ІТ-сервісів Тема 2.5. Моніторинг та резервне копіювання
9.	Запланована навчальна діяльність та методи навчання	Навчальна діяльність здійснюється шляхом лекційних, практичних занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій.
10.	Методи і критерії оцінювання	Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, екзамен. Рівень підготовки студентів оцінюється наступним чином: “*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок; “*Дуже добре*” (B) – вище середнього рівня з кількома помилками; “*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок; “*Задовільно*” (D) – непогано, але зі значною кількістю недоліків; “*Достатньо*” (E) – виконання задовольняє

		мінімальні критерії; “*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку; “*Незадовільно*” (F) – необхідна серйозна подальша робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра кібербезпеки центру кібербезпеки
Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій

Додаток 12

Каталог освітнього компонента

№ з/п	Назва складової каталогу	Зміст
1.	Галузь знань	К Безпека та оборона
1.1.	Спеціальність	К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
1.2.	Рівень вищої освіти	Другий (магістерський)
2.	Назва навчальної дисципліни	**ОК-12. Кіберзахист об'єктів критичної інфраструктури**
3.	Тип навчальної дисципліни (спецкурсу) (обов'язкова або вибіркова, спеціалізація)	Обов'язкова
4.	Курс (семестр), у якому вивчається	1(2) денна форма, 2(3) заочна форма
5.	Необхідні обов'язкові попередні та супутні навчальні дисципліни (спецкурси), у тому числі розділи, теми таких дисциплін, спецкурсів, модулів	«Методологія наукових досліджень та академічна доброчесність», «Організаційно-правове забезпечення кіберзахисту», «Системне адміністрування та організація безпеки ІТ-сервісів»
6.	Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах	**6 ЄКТС/ 180 год.**, зокрема для: - лекційних занять – 38 год. / 10 год. (заочна); - практичних (лабораторних) занять – 38 год. / 14 год. (заочна); - самостійної роботи – 104 год. / 156 год. (заочна)
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності. ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН 12. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки і є основою для прийняття ефективних рішень, проведення досліджень та критичного осмислення проблем у галузі національної безпеки. ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення ПРН 22. Оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації

		ПРН 26. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Змістовний модуль І. Технологічні підходи щодо інформаційної безпеки об'єктів критичної інфраструктури Тема 1.1. Вимоги до кіберзахисту об'єктів критичної інфраструктури Тема 1.2. Політика інформаційної безпеки на об'єктах критичної інфраструктури Тема 1.3. Доступ користувачів до об'єктів критичної інфраструктури Тема 1.4. Ідентифікація та автентифікація користувачів об'єкта критичної інфраструктури Тема 1.5. Реєстрація подій та аудит об'єкта критичної інфраструктури Змістовний модуль ІІ. Мережевий захист компонентів та інформаційних ресурсів об'єктів критичної інформаційної інфраструктури Тема 2.1. Мережевий захист об'єктів критичної інформаційної інфраструктури Тема 2.2. Апаратні та програмні засоби мережевого захисту об'єктів критичної інформаційної інфраструктури Тема 2.3.Аналіз захищеності мережевих об'єктів критичної інфраструктури Тема 2.4. Використання бездротових мереж на об'єктах критичної інфраструктури Змістовний модуль ІІІ. Системи захисту від витоку даних Тема 3.1. Системи DLP: принцип дії, політики, контроль витоку даних Тема 3.2. Сучасні DLP: Safetica, Symantec DLP, Endpoint Protector Змістовний модуль IV. Курсова робота
	Запланована навчальна діяльність та методи навчання	Навчальна діяльність здійснюється шляхом лекційних, практичних занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій.
10.	Методи і критерії оцінювання	Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, курсова робота, екзамен. Рівень підготовки студентів оцінюється наступним чином: "*Відмінно*" (А) – відмінне виконання лише з незначною кількістю помилок; "*Дуже добре*" (В) – вище середнього рівня з

		кількома помилками; “*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок; “*Задовільно*” (D) – непогано, але зі значною кількістю недоліків; “*Достатньо*” (E) – виконання задовольняє мінімальні критерії; “*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку; “*Незадовільно*” (F) – необхідна серйозна подальша робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра кібербезпеки центру кібербезпеки
Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій

Додаток 13

Каталог освітнього компонента

№ з/п	Назва складової каталогу	Зміст
1.	Галузь знань	К Безпека та оборона
1.1.	Спеціальність	К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
1.2.	Рівень вищої освіти	Другий (магістерський)
2.	Назва навчальної дисципліни	**ОК-13. Аудит інформаційної безпеки та кібербезпеки**
3.	Тип навчальної дисципліни (спецкурсу) (обов'язкова або вибіркова, спеціалізація)	Обов'язкова
4.	Курс (семестр), у якому вивчається	2 (3)
5.	Необхідні обов'язкові попередні та супутні навчальні дисципліни (спецкурси), у тому числі розділи, теми таких дисциплін, спецкурсів, модулів	«Актуальні проблеми інформаційної безпеки», «Кіберзахист об'єктів критичної інфраструктури», «Організаційно-правове забезпечення кіберзахисту»
6.	Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах	**4 ЄКТС/ 120 год.**, зокрема для: - лекційних занять – 14 год. / 6 год (заочна); - семінарських занять – 30 год. / 8 год. (заочна); - самостійної роботи – 76 год. / 106 год. (заочна)
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (кіберзахист, забезпечення державної безпеки в інформаційній сфері), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог. ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН 18. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. ПРН 19. Аналізувати та оцінювати захищеність

		систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення ПРН 21. Досліджувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури ПРН 22. Оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації ПРН 26. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Модуль І. Основи аудиту кібернетичної безпеки 1.1. Поняття аудиту кібернетичної безпеки 1.2. Методи та процеси аудиту кібернетичної безпеки Модуль ІІ. Організація проведення аудиту кібернетичної безпеки. 2.1. Етапи аудиту кібернетичної безпеки
9.	Запланована навчальна діяльність та методи навчання	Навчальна діяльність здійснюється шляхом лекційних, семінарських занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій.
10.	Методи і критерії оцінювання	Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, екзамен. Рівень підготовки студентів оцінюється наступним чином: "*Відмінно*" (A) – відмінне виконання лише з незначною кількістю помилок; "*Дуже добре*" (B) – вище середнього рівня з кількома помилками; "*Добре*" (C) – у загальному правильна робота з певною кількістю грубих помилок; "*Задовільно*" (D) – непогано, але зі значною кількістю недоліків; "*Достатньо*" (E) – виконання задовольняє мінімальні критерії; "*Незадовільно*" (FX) – потрібно працювати перед тим, як отримати позитивну оцінку; "*Незадовільно*" (F) – необхідна серйозна подальша робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра кібербезпеки центру кібербезпеки
Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій

Додаток 14

Каталог освітнього компонента

№ з/п	Назва складової каталогу	Зміст
1.	Галузь знань	К Безпека та оборона
1.1.	Спеціальність	К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
1.2.	Рівень вищої освіти	Другий (магістерський)
2.	Назва навчальної дисципліни	**ОК-14. Управління кіберінцидентами**
3.	Тип навчальної дисципліни (спецкурсу) (обов'язкова або вибіркова, спеціалізація)	Обов'язкова
4.	Курс (семестр), у якому вивчається	2 (3) денна форма, 2(4) заочна форма
5.	Необхідні обов'язкові попередні та супутні навчальні дисципліни (спецкурси), у тому числі розділи, теми таких дисциплін, спецкурсів, модулів	«Актуальні проблеми інформаційної безпеки», «Розвідка з відкритих джерел інформації OSINT», «Іноземна мова професійного спрямування», «Кіберзахист об'єктів критичної інфраструктури»
6.	Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах	**6 ЄКТС/180 год.**, зокрема для: - лекційних занять – 30 год. / 10 год. (заочна); - семінарських занять – 30 год. / 14 год. (заочна); - самостійної роботи – 120 год. / 156 год. (заочна)
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (кіберзахист, забезпечення державної безпеки в інформаційній сфері), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог. ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН 16. Організовувати та спрямовувати діяльність фахівців з кіберзахисту у сфері інформаційних технологій та кіберпросторі; розробляти та впроваджувати заходи із кіберзахисту у сфері інформаційних технологій та кіберпросторі, самостійно та у взаємодії з контролюючими органами. ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту,

		технології створення та використання спеціалізованого програмного забезпечення. ПРН 22. Оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації ПРН 23. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ПРН 26. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Модуль І. Основи управління кіберінцидентами Тема .1.1. Поняття кіберінциденту. Найвідоміші кіберінциденти в Україні та світі Тема 1.2. Категоризація кіберінцидентів Тема 1.3. Етапи процесу управління кіберінцидентами Модуль ІІ. Реагування на кіберінциденти Тема 2.1. Класифікація вразливостей інформаційних систем Тема 2.2. Моніторинг подій інформаційної безпеки Тема 2.3. Засоби реагування на кіберінциденти Тема 2.4. Аналіз інцидентів та цифрова криміналістика
9.	Запланована навчальна діяльність та методи навчання	Навчальна діяльність здійснюється шляхом лекційних, семінарських занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій.
10.	Методи і критерії оцінювання	Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, екзамен. Рівень підготовки студентів оцінюється наступним чином: “*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок; “*Дуже добре*” (B) – вище середнього рівня з кількома помилками; “*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок; “*Задовільно*” (D) – непогано, але зі значною кількістю недоліків; “*Достатньо*” (E) – виконання задовольняє мінімальні критерії; “*Незадовільно*” (FX) – потрібно працювати перед

		тим, як отримати позитивну оцінку; “*Незадовільно*” (F) – необхідна серйозна подальша робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра кібербезпеки центру кібербезпеки
Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій

Додаток 15

Каталог освітнього компонента

№ з/п	Назва складової каталогу	Зміст
1.	Галузь знань	К Безпека та оборона
1.1.	Спеціальність	К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
1.2.	Рівень вищої освіти	Другий (магістерський)
2.	Назва навчальної дисципліни	**ОК-15. Методи і моделі протидії кіберзагрозам**
3.	Тип навчальної дисципліни (спецкурсу) (обов'язкова або вибіркова, спеціалізація)	Обов'язкова
4.	Курс (семестр), у якому вивчається	2(3)
5.	Необхідні обов'язкові попередні та супутні навчальні дисципліни (спецкурси), у тому числі розділи, теми таких дисциплін, спецкурсів, модулів	«Методологія наукових досліджень та академічна доброчесність», «Іноземна мова професійного спрямування», «Теорія прийняття рішень і управління», «Прикладні системи штучного інтелекту в кіберпросторі», «Організаційно-правове забезпечення кіберзахисту», «Системне адміністрування та організація безпеки ІТ-сервісів»
6.	Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах	**5 ЄКТС/ 150 год.**, зокрема для: - лекційних занять –30 год. / 8 год. (заочна); - практичних (лабораторних) занять – 30 год. / 8 год (заочна); - самостійної роботи – 90 год. / 134 год. (заочна)
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності. ПРН 4. Організовувати роботу колективу, забезпечувати професійний розвиток його членів та досягнення поставлених цілей. ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів. ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення ПРН 21. Досліджувати системи та засоби

		інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури ПРН 22. Оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації ПРН 25. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Змістовний модуль 1. Методи виявлення та аналізу кіберзагроз Тема 1.1. Класифікація кіберзагроз. Життєвий цикл кіберзагроз та кібератак Тема 1.2. Методи маскування та шифрування даних Тема 1.3. Стратегії здійснення кібератак. Методи боротьби з DDoS-атаками Тема 1.4. Моделювання та прогнозування кіберзагроз Тема 1.5. Моніторинг та основи діагностики комп’ютерних мереж, рбота з утилітами Linux Kali Змістовний модуль ІІ. Сервіси для організації протидії кіберзагрозам Тема 2.1. Методи маскування та шифрування даних Тема 2.2. Методи захисту кінцевих точок в комп’ютерних мережах Тема 2.3. Інструменти та практики протидії кіберзагрозам
	Запланована навчальна діяльність та методи навчання	Навчальна діяльність здійснюється шляхом лекційних, практичних занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій.
10.	Методи і критерії оцінювання	Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, екзамен. Рівень підготовки студентів оцінюється наступним чином: “*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок; “*Дуже добре*” (B) – вище середнього рівня з кількома помилками; “*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок; “*Задовільно*” (D) – непогано, але зі значною кількістю недоліків; “*Достатньо*” (E) – виконання задовольняє мінімальні критерії; “*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;

		“*Незадовільно*” (F) – необхідна серйозна подальша робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра кібербезпеки центру кібербезпеки
Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій

Додаток 16

Каталог освітнього компонента

№ з/п	Назва складової каталогу	Зміст
1.	Галузь знань	К Безпека та оборона
1.1.	Спеціальність	К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
1.2.	Рівень вищої освіти	Другий (магістерський)
2.	Назва навчальної дисципліни	**ОК-16. Безпека розподілених інформаційних ресурсів та хмарні технології**
3.	Тип навчальної дисципліни (спецкурсу) (обов'язкова або вибіркова, спеціалізація)	Обов'язкова
4.	Курс (семестр), у якому вивчається	2(4)
5.	Необхідні обов'язкові попередні та супутні навчальні дисципліни (спецкурси), у тому числі розділи, теми таких дисциплін, спецкурсів, модулів	«Теорія прийняття рішень і управління», «Організаційно-правове забезпечення кіберзахисту», «Іноземна мова професійного спрямування», «Методи і моделі протидії кіберзагрозам», «Кіберзахист об'єктів критичної інфраструктури»
6.	Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах	**4 ЄКТС/ 120 год.**, зокрема для: - лекційних занять – 20 год. / 6 год (заочна); - практичних (лабораторних) занять – 20 год. / 8 год. (заочна); - самостійної роботи – 80 год. / 106 год (заочна)
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН 9. Синтезувати спектр заходів та підходів, що можуть використовуватись для вирішення проблем, пов'язаних з викликами глобальній, європейській та регіональній безпеці. ПРН 18. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. ПРН 21. Досліджувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної

		інфраструктури ПРН 23. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ПРН 24. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Модуль І. Безпека розподілених інформаційних ресурсів та хмарні обчислення Тема 1. Розподілені обчислювальні системи та основи хмарних обчислень. Тема 2. Технологічні основи хмарних обчислень. Тема 3. Захист інформації під час використання хмарних сервісів Тема 4. Протидія загрозам у сфері розподілених систем
	Запланована навчальна діяльність та методи навчання	Навчальна діяльність здійснюється шляхом лекційних, практичних занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій.
10.	Методи і критерії оцінювання	Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, екзамен. Рівень підготовки студентів оцінюється наступним чином: “*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок; “*Дуже добре*” (B) – вище середнього рівня з кількома помилками; “*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок; “*Задовільно*” (D) – непогано, але зі значною кількістю недоліків; “*Достатньо*” (E) – виконання задовольняє мінімальні критерії; “*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку; “*Незадовільно*” (F) – необхідна серйозна подальша робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра безпеки інформаційно-комунікаційних систем центру кібербезпеки
Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій

Додаток 17

Каталог освітнього компонента

№ з/п	Назва складової каталогу	Зміст
1.	Галузь знань	К Безпека та оборона
1.1.	Спеціальність	К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
1.2.	Рівень вищої освіти	Другий (магістерський)
2.	Назва навчальної дисципліни	**ОК-17. Кіберзахист інформаційних систем сектору безпеки та оборони держави**
3.	Тип навчальної дисципліни (спецкурсу) (обов'язкова або вибіркова, спеціалізація)	Обов'язкова
4.	Курс (семестр), у якому вивчається	2 (4)
5.	Необхідні обов'язкові попередні та супутні навчальні дисципліни (спецкурси), у тому числі розділи, теми таких дисциплін, спецкурсів, модулів	«Актуальні проблеми інформаційної безпеки», «Організаційно-правове забезпечення кіберзахисту», «Іноземна мова професійного спрямування», «Методи і моделі протидії кіберзагрозам», «Кіберзахист об'єктів критичної інфраструктури», «Системне адміністрування та організація безпеки ІТ-сервісів»
6.	Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах	**4 ЄКТС/ 120 год.**, зокрема для: - лекційних занять – 30 год. / 8 год. (заочна); - семінарських занять – 30 год. / 6 год (заочна); - самостійної роботи – 60 год. / 106 год. (заочна)
7.	Програмні результати навчання	ПРН 3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (кіберзахист, забезпечення державної безпеки в інформаційній сфері), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог. ПРН 10. Формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності) (кіберзахист, забезпечення державної безпеки в інформаційній сфері). ПРН 13. Організовувати та здійснювати керівництво територіальною обороною, мобілізаційною підготовкою та мобілізацією у межах професійної компетентності. ПРН 14. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються. ПРН 18. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному

		рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Модуль І. Встановлення та розгортання систем управління базами даних на системах сектору безпеки та оборони держави Тема 1.1. Види та класифікація систем управління базами даних Тема 1.2. Методологічні основи проєктування баз даних Тема 1.3. Розгортання СУБД Тема 1.4. СУБД нового покоління Тема 1.5. Рольові моделі доступу в СУБД Тема 1.6. Захист та безпека баз даних Тема 1.7. Резервне копіювання та відновлення баз даних Тема 1.8. Інструменти тестування та моніторингу роботи СУБД Модуль ІІ. Засоби організації кіберзахисту інформаційних систем сектору безпеки та оборони держави Тема 2.1. Криптографічні засоби захисту інформації Тема 2.2. управління кіберризиками Тема 2.3. Кібервійна Тема 2.4. Організаційні та технічні аспекти кіберзахисту
9.	Запланована навчальна діяльність та методи навчання	Навчальна діяльність здійснюється шляхом лекційних, семінарських занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій.
10.	Методи і критерії оцінювання	Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, екзамен. Рівень підготовки студентів оцінюється наступним чином: “*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок; “*Дуже добре*” (B) – вище середнього рівня з кількома помилками; “*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок; “*Задовільно*” (D) – непогано, але зі значною кількістю недоліків; “*Достатньо*” (E) – виконання задовольняє мінімальні критерії; “*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;

		“*Незадовільно*” (F) – необхідна серйозна подальша робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра кібербезпеки центру кібербезпеки
Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій

Додаток 18

Каталог освітнього компонента

№ з/п	Назва складової каталогу	Зміст
1.	Галузь знань	К Безпека та оборона
1.1.	Спеціальність	К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
1.2.	Рівень вищої освіти	Другий (магістерський)
2.	Назва навчальної дисципліни	**ОК-18. Науково-дослідна практика**
3.	Тип навчальної дисципліни (спецкурсу) (обов'язкова або вибіркова, спеціалізація)	Обов'язкова
4.	Курс (семестр), у якому вивчається	2 (4) – денна форма, 3(5) – заочна форма
5.	Необхідні обов'язкові попередні та супутні навчальні дисципліни (спецкурси), у тому числі розділи, теми таких дисциплін, спецкурсів, модулів	«Методологія наукових досліджень та академічна доброчесність», «Теорія прийняття рішень і управління», «Іноземна мова професійного спрямування», «Гендерна політика в секторі безпеки та оборони України», «Системне адміністрування та організація безпеки IT-сервісів», «Інформаційне протиборство», «Прикладні системи штучного інтелекту в кіберпросторі», «Організаційно-правове забезпечення кіберзахисту», «Актуальні проблеми інформаційної безпеки», «Розвідка з відкритих джерел інформації (OSINT)», «Методи і моделі протидії кіберзагрозам», «Кіберзахист об'єктів критичної інфраструктури», «Управління кіберінцидентами», «Аудит інформаційної безпеки та кібербезпеки», «Безпека розподілених інформаційних ресурсів та хмарні технології», «Кіберзахист інформаційних систем сектору безпеки та оборони держави»
6.	Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах	**9 ЄКТС/ 270 год.**, зокрема для: - самостійної роботи – 270 год.
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності. ПРН 3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (кіберзахист, забезпечення державної безпеки в інформаційній сфері), у тому числі в умовах

		багатокритеріальності, неповних чи суперечливих інформації та вимог. ПРН 4. Організовувати роботу колективу, забезпечувати професійний розвиток його членів та досягнення поставлених цілей. ПРН 5. Розробляти та реалізовувати інноваційні проєкти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів. ПРН 6. Вільно спілкуватися державною та іноземною мовами усно і письмово для обговорення професійної діяльності, результатів досліджень та інновацій, пошуку та аналізу відповідної інформації. ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН 9. Синтезувати спектр заходів та підходів, що можуть використовуватись для вирішення проблем, пов'язаних з викликами глобальній, європейській та регіональній безпеці. ПРН 10. Формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності) (кіберзахист, забезпечення державної безпеки в інформаційній сфері). ПРН 11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання професійних задач у визначених законодавством сферах та за напрямами майбутньої діяльності. ПРН 12. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки і є основою для прийняття ефективних рішень, проведення досліджень та критичного осмислення проблем у галузі національної безпеки. ПРН 13. Організовувати та здійснювати керівництво територіальною обороною, мобілізаційною підготовкою та мобілізацією у межах професійної компетентності. ПРН 14. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються. ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів. ПРН 17. Створювати та документально оформлювати організаційно-технічні та організаційно-правові моделі кіберзахисту, а також моделі захисту конфіденційності, організовувати та розробляти системи кіберзахисту у сфері інформаційних технологій та кіберпростору,

		здійснювати моніторинг та аудит інформаційної безпеки та кібербезпеки на підприємствах, установах та організаціях різних форм власності. ПРН 18. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення ПРН 20. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН 21. Досліджувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури ПРН 22. Оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації ПРН 23. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ПРН 24. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. ПРН 25. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Змістовний модуль 1. Науково-дослідна практика Тема 1. Розробка індивідуального графіку проходження практики. Узгодження його з науковим керівником кваліфікаційної (магістерської) роботи та керівником практики від кафедри. Тема 2. Визначення предмету та об'єкту дослідження, мети та завдань дослідження відповідно до закріпленої

		за здобувачем теми кваліфікаційної (магістерської) роботи Тема 3. Ознайомлення з науковими напрямами роботи на базі практики Тема 4. Ознайомлення з іноземними та вітчизняними науково-інформаційними джерелами за спеціалізацією, обрання наукової проблематики та формування бібліографії Тема 5. Збір та обробка даних щодо стану об'єкту дослідження на базі практики. Тема 6. Ознайомлення з нормативно-правовою документацією за обраною проблематикою та формування напрямів удосконалення стану об'єкту дослідження. Тема 7. Виконання індивідуального завдання відповідно до теми кваліфікаційної (магістерської) роботи Тема 8. Написання звіту з науково-дослідної практики
	Запланована навчальна діяльність та методи навчання	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.
10.	Методи і критерії оцінювання	Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, диференційований залік. Рівень підготовки студентів оцінюється наступним чином: "*Відмінно*" (A) – відмінне виконання лише з незначною кількістю помилок; "*Дуже добре*" (B) – вище середнього рівня з кількома помилками; "*Добре*" (C) – у загальному правильна робота з певною кількістю грубих помилок; "*Задовільно*" (D) – непогано, але зі значною кількістю недоліків; "*Достатньо*" (E) – виконання задовольняє мінімальні критерії; "*Незадовільно*" (FX) – потрібно працювати перед тим, як отримати позитивну оцінку; "*Незадовільно*" (F) – необхідна серйозна подальша робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра кібербезпеки центру кібербезпеки
Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій

Додаток 19

Каталог освітнього компонента

№ з/п	Назва складової каталогу	Зміст
1.	Галузь знань	К Безпека та оборона
1.1.	Спеціальність	К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
1.2.	Рівень вищої освіти	Другий (магістерський)
2.	Назва навчальної дисципліни	**ОК-19. Кваліфікаційна (магістерська) робота**
3.	Тип навчальної дисципліни (спецкурсу) (обов'язкова або вибіркова, спеціалізація)	Обов'язкова
4.	Курс (семестр), у якому вивчається	2 (4) – денна форма, 3(5) – заочна форма
5.	Необхідні обов'язкові попередні та супутні навчальні дисципліни (спецкурси), у тому числі розділи, теми таких дисциплін, спецкурсів, модулів	«Методологія наукових досліджень та академічна доброчесність», «Теорія прийняття рішень і управління», «Іноземна мова професійного спрямування», «Гендерна політика в секторі безпеки та оборони України», «Системне адміністрування та організація безпеки IT-сервісів», «Інформаційне протиборство», «Прикладні системи штучного інтелекту в кіберпросторі», «Організаційно-правове забезпечення кіберзахисту», «Актуальні проблеми інформаційної безпеки», «Розвідка з відкритих джерел інформації (OSINT)», «Методи і моделі протидії кіберзагрозам», «Кіберзахист об'єктів критичної інфраструктури», «Управління кіберінцидентами», «Аудит інформаційної безпеки та кібербезпеки», «Безпека розподілених інформаційних ресурсів та хмарні технології», «Кіберзахист інформаційних систем сектору безпеки та оборони держави»
6.	Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах	**6 ЄКТС/180 год.**, зокрема для: - самостійної роботи – 180 год.
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності. ПРН 3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (кіберзахист, забезпечення державної безпеки в інформаційній сфері), у тому числі в умовах

		багатокритеріальності, неповних чи суперечливих інформації та вимог. ПРН 4. Організовувати роботу колективу, забезпечувати професійний розвиток його членів та досягнення поставлених цілей. ПРН 5. Розробляти та реалізовувати інноваційні проєкти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів. ПРН 6. Вільно спілкуватися державною та іноземною мовами усно і письмово для обговорення професійної діяльності, результатів досліджень та інновацій, пошуку та аналізу відповідної інформації. ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН 9. Синтезувати спектр заходів та підходів, що можуть використовуватись для вирішення проблем, пов'язаних з викликами глобальній, європейській та регіональній безпеці. ПРН 10. Формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності) (кіберзахист, забезпечення державної безпеки в інформаційній сфері). ПРН 11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання професійних задач у визначених законодавством сферах та за напрямами майбутньої діяльності. ПРН 12. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки і є основою для прийняття ефективних рішень, проведення досліджень та критичного осмислення проблем у галузі національної безпеки. ПРН 13. Організовувати та здійснювати керівництво територіальною обороною, мобілізаційною підготовкою та мобілізацією у межах професійної компетентності. ПРН 14. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються. ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів. ПРН 17. Створювати та документально оформлювати організаційно-технічні та організаційно-правові моделі кіберзахисту, а також моделі захисту конфіденційності, організовувати та розробляти системи кіберзахисту у сфері інформаційних технологій та кіберпростору,

		здійснювати моніторинг та аудит інформаційної безпеки та кібербезпеки на підприємствах, установах та організаціях різних форм власності. ПРН 18. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення ПРН 20. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН 21. Досліджувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури ПРН 22. Оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації ПРН 23. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ПРН 24. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. ПРН 25. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Теми кваліфікаційних (магістерських) робіт затверджуються Наказом Національної академії Служби безпеки України.
9.	Запланована навчальна діяльність та методи навчання	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез,

		індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.
10.	Методи і критерії оцінювання	Методами контролю є: публічний захист кваліфікаційних (магістерських) робіт. Рівень підготовки студентів оцінюється наступним чином: “*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок; “*Дуже добре*” (B) – вище середнього рівня з кількома помилками; “*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок; “*Задовільно*” (D) – непогано, але зі значною кількістю недоліків; “*Достатньо*” (E) – виконання задовольняє мінімальні критерії; “*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку; “*Незадовільно*” (F) – необхідна серйозна подальша робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра кібербезпеки центру кібербезпеки
Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій