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 | 25 Воєнні науки, національна безпека, безпека державного кордону |
| 1.1. | Спеціальність | 256 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:<br>- лекційних занять – 12 год. / 8 год. (заочна);<br>- семінарських занять – 10 год. / 4 год. (заочна);<br>- практичних (лабораторних) занять – 10 год. / 2 год. (заочна);<br>- самостійної роботи – 58 год. / 76 год (заочна). |
| 7. | Програмні результати навчання | ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.<br>ПРН 5. Розробляти та реалізовувати інноваційні проєкти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів.<br>ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.<br>ПРН 11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання професійних задач у визначених законодавством сферах та за напрямами майбутньої діяльності.<br>ПРН 14. Зрозуміло і недвозначно доносити власні |

| | | |
|---|---|---|
| | | знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються.<br>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.<br>Тема 1. Система організації та управління науковими дослідженнями в Україні. Академічна доброчесність<br>Тема 2. Методологія наукових досліджень та її значення у науковій роботі.<br>Тема 3. Загальнонаукові методи дослідження / Градація методів наукового дослідження (заочна)<br>Змістовний модуль 2. Теорія та практика наукових досліджень.<br>Тема 1. Основи когнітивної творчості дослідника / Магістерська праця: характеристика, етапи проведення, сучасні вимоги (заочна)<br>Тема 2. Підготовка публікацій, доповідей і повідомлень на наукових заходах.<br>Тема 3. Оформлення і захист результатів дослідження. |
| 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.<br>Рівень підготовки студентів оцінюється наступним чином:<br>“*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок;<br>“*Дуже добре*” (B) – вище середнього рівня з кількома помилками;<br>“*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок;<br>“*Задовільно*” (D) – непогано, але зі значною кількістю недоліків;<br>“*Достатньо*” (E) – виконання задовольняє мінімальні критерії;<br>“*Незадовільно*” (FX) – потрібно працювати перед |

| | | |
|---|---|---|
| | | тим, як отримати позитивну оцінку;<br>“*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 | 25 Воєнні науки, національна безпека, безпека державного кордону |
| 1.1. | Спеціальність | 256 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:<br>- лекційних занять – 12 год. / 8 год. (заочна);<br>- семінарських занять – 20 год. / 6 год. (заочна);<br>- самостійної роботи – 58 год. / 76 год (заочна). |
| 7. | Програмні результати навчання | ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.<br>ПРН 6. Вільно спілкуватися державною та іноземною мовами усно і письмово для обговорення професійної діяльності, результатів досліджень та інновацій, пошуку та аналізу відповідної інформації.<br>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<br>1. Специфіка наукового тексту й професійного наукового викладу думки<br>2. Морфологічні норми фахового наукового мовлення професіонала з організації |

| | | |
|---|---|---|
| | | інформаційної безпеки<br>3. Синтаксичні норми фахового наукового мовлення професіонала з організації інформаційної безпеки<br>4. Укладання фахового публічного виступу професіонала з організації інформаційної безпеки<br>5. Мистецтво виголошення фахового публічного виступу професіонала з організації інформаційної безпеки. Мовна поведінка оратора.<br>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.<br>Рівень підготовки студентів оцінюється наступним чином:<br>“*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок;<br>“*Дуже добре*” (B) – вище середнього рівня з кількома помилками;<br>“*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок;<br>“*Задовільно*” (D) – непогано, але зі значною кількістю недоліків;<br>“*Достатньо*” (E) – виконання задовольняє мінімальні критерії;<br>“*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;<br>“*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 | 25 Воєнні науки, національна безпека, безпека державного кордону |
| 1.1. | Спеціальність | 256 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** |
| 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:<br>- лекційних занять – 12 год. / 8 год. (заочна);<br>- семінарських занять – 10 год. / 4 год. (заочна);<br>- практичних (лабораторних) занять – 10 год. / 2 год. (заочна);<br>- самостійної роботи – 58 год. / 76 год (заочна). |
| 7. | Програмні результати навчання | ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.<br>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.<br>ПРН 4. Організовувати роботу колективу, забезпечувати професійний розвиток його членів та досягнення поставлених цілей.<br>ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.<br>ПРН 11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання |

| | | |
|---|---|---|
| | | професійних задач у визначених законодавством сферах та за напрямами майбутньої діяльності.<br>ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів.<br>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.<br>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. Основи теорії прийняття рішень<br>Тема 1.1. Основи теорії прийняття рішень.<br>Тема 1.2. Невизначеності в теорії прийняття рішень<br>Модуль ІІ. Методи та моделі в теорії прийняття рішень<br>Тема 2.1. Методи прийняття рішень<br>Тема 2.2. Моделювання в теорії прийняття рішень |
| 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.<br>Рівень підготовки студентів оцінюється наступним чином:<br>“*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок;<br>“*Дуже добре*” (B) – вище середнього рівня з кількома помилками;<br>“*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок;<br>“*Задовільно*” (D) – непогано, але зі значною кількістю недоліків;<br>“*Достатньо*” (E) – виконання задовольняє мінімальні критерії;<br>“*Незадовільно*” (FX) – потрібно працювати перед |

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

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

Додаток 4

Каталог освітнього компонента

| № з/п | Назва складової каталогу | Зміст |
|---|---|---|
| 1. | Галузь знань | 25 Воєнні науки, національна безпека, безпека державного кордону |
| 1.1. | Спеціальність | 256 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:<br>- практичних (лабораторних) занять – 88 год. / 24 год (заочна);<br>- 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.<br>ПРН 6. Вільно спілкуватися державною та іноземною мовами усно і письмово для обговорення професійної діяльності, результатів досліджень та інновацій, пошуку та аналізу відповідної інформації.<br>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.<br>Тема 1. Типи інформаційних джерел.<br>Тема 2. Аналіз наукової літератури професійного спрямування.<br>Тема 3. Типи інформації. Основні характеристики. |

| | | |
|---|---|---|
| | | Модуль ІІ. Інформаційна безпека.<br>Тема 1. Основні засади інформаційної безпеки.<br>Тема 2. Основні загрози інформаційній безпеці.<br>Тема 3. Захист інформації, методи і способи протидії основним загрозам.<br>Модуль ІІІ. Стратегії успішного працевлаштуванні.<br>Тема 1. Підготовка необхідних форм документації для успішного працевлаштування.<br>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.<br>Рівень підготовки студентів оцінюється наступним чином:<br>“*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок;<br>“*Дуже добре*” (B) – вище середнього рівня з кількома помилками;<br>“*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок;<br>“*Задовільно*” (D) – непогано, але зі значною кількістю недоліків;<br>“*Достатньо*” (E) – виконання задовольняє мінімальні критерії;<br>“*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;<br>“*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 | 25 Воєнні науки, національна безпека, безпека державного кордону |
| 1.1. | Спеціальність | 256 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 системі національної 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:<br>- лекційних занять – 10 год. / 6 год (заочна);<br>- семінарських занять – 20 год. / 6 год (заочна);<br>- 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.<br>ПРН 8. Забезпечувати дотримання принципу гендерної рівності під час здійснення професійної діяльності.<br>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.<br>Тема 1. Поняття гендер, гендерна рівність, гендерна чутливість у суспільно-політичному та науковому дискурсах. Міжнародно-правове забезпечення гендерної рівності. Українське законодавство щодо гендерних питань<br>Тема 2. Гендерно чутливі комунікації в секторі безпеки і оборони. Передумова, наслідки і протидія |

| | | |
|---|---|---|
| | | дискримінації за ознакою статі.<br>Модуль ІІ. Урахування гендерних підходів у діяльності з питань запобігання шкоди цивільному населенню в умовах бойових дій.<br>Тема 1. Гендерний компонент інформаційно-психологічних заходів.<br>Тема 2. Збирання первинних доказів сексуального насильства в умовах війни |
| 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.<br>Рівень підготовки студентів оцінюється наступним чином:<br>“*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок;<br>“*Дуже добре*” (B) – вище середнього рівня з кількома помилками;<br>“*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок;<br>“*Задовільно*” (D) – непогано, але зі значною кількістю недоліків;<br>“*Достатньо*” (E) – виконання задовольняє мінімальні критерії;<br>“*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;<br>“*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 | 25 Воєнні науки, національна безпека, безпека державного кордону |
| 1.1. | Спеціальність | 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) |
| 1.3. | Рівень вищої освіти | Другий (магістерський) |
| 2. | Назва навчальної дисципліни | **ОК-6. Теорія кіберпростору, кібербезпеки та 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 | **4 ЄКТС/ 120 год.**, зокрема для:<br>- лекційних занять – 22 год. / 6 год. (заочна);<br>- семінарських занять – 22 год. / 8 год. (заочна);<br>- самостійної роботи – 76 год. / 106 год (заочна) |
| 7. | Програмні результати навчання | ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.<br>ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.<br>ПРН 10. Формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності) (кіберзахист, забезпечення державної безпеки в інформаційній сфері).<br>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.<br>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.<br>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. Основи теорії кіберпростору.<br>Тема 1. Основні положення та визначення кіберпростору.<br>Тема 2. Основні напрями розвитку теорії кіберпростору.<br>Тема 3. Основи спілкування у кіберпросторі.<br>Тема 4. Основи економіки кіберпростору.<br>Тема 5. Основні напрями розвитку гуманітарних наук у кіберпросторі.<br>Модуль 2. Основи кібербезпеки<br>Тема 6. Основні напрями розвитку теорії і практики кібербезпеки у контексті забезпечення національної безпеки та безпеки держави.<br>Тема 7. Основні підходи до визначення видів протиборства в інформаційній сфері та кіберпросторі.<br>Тема 8. Війна як один із способів протиборства в інформаційній сфері та кіберпросторі.<br>Тема 9. Основи теорії і практики щодо розробки технології забезпечення кібербезпеки<br>Модуль 3. Основи кіберзахисту<br>Тема 10. Теоретичні основи щодо створення архітектури захисту кіберпростору. |
| 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.<br>Рівень підготовки студентів оцінюється наступним чином:<br>“*Відмінно*” (А) – відмінне виконання лише з незначною кількістю помилок;<br>“*Дуже добре*” (В) – вище середнього рівня з кількома помилками; |

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

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

Додаток 7

Каталог освітнього компонента

| № з/п | Назва складової каталогу | Зміст |
|---|---|---|
| 1. | Галузь знань | 25 Воєнні науки, національна безпека, безпека державного кордону |
| 1.1. | Спеціальність | 256 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:<br>- лекційних занять – 22 год. / 8 год. (заочне);<br>- семінарських занять – 32 год. / 8 год. (заочне);<br>- 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.<br>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.<br>ПРН 5. Розробляти та реалізовувати інноваційні проєкти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів.<br>ПРН 8. Забезпечувати дотримання принципу гендерної рівності під час здійснення професійної діяльності.<br>ПРН 11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання |

| | | |
|---|---|---|
| | | професійних задач у визначених законодавством сферах та за напрямами майбутньої діяльності.<br>ПРН 13. Організовувати та здійснювати керівництво територіальною обороною, мобілізаційною підготовкою та мобілізацією у межах професійної компетентності.<br>ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів.<br>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.<br>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.<br>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<br>Тема 1. Генезис інформаційного протиборства<br>Тема 2. Сучасні стратегії та концепції інформаційного протиборства<br>Змістовий модуль ІІ. Теоретичні та технологічні основи інформаційного протиборства<br>Тема 3. Теоретичні основи інформаційного протиборства<br>Тема 4. Технології та засоби інформаційного протиборства<br>Змістовий модуль ІІІ. Організаційні аспекти підготовки та ведення інформаційного протиборства<br>Тема 5. Форми ведення інформаційного протиборства<br>Тема 6. Підготовка та ведення інформаційного протиборства з використанням соціально-орієнтованих ресурсів мережі Internet та відкритих даних<br>Тема 7. Перспективи ведення інформаційного |

| | | |
|---|---|---|
| | | протиборства в соціальних мережах |
| | 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.<br>Рівень підготовки студентів оцінюється наступним чином:<br>“*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок;<br>“*Дуже добре*” (B) – вище середнього рівня з кількома помилками;<br>“*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок;<br>“*Задовільно*” (D) – непогано, але зі значною кількістю недоліків;<br>“*Достатньо*” (E) – виконання задовольняє мінімальні критерії;<br>“*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;<br>“*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 | 25 Воєнні науки, національна безпека, безпека державного кордону |
| 1.1. | Спеціальність | 256 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:<br>- лекційних занять – 22 год. / 6 год. (заочна);<br>- практичних (лабораторних) занять – 22 год. / 8 год. (заочна);<br>- самостійної роботи – 76 год. / 106 год. (заочна) |
| 7. | Програмні результати навчання | ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.<br>ПРН 10. Формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності) (кіберзахист, забезпечення державної безпеки в інформаційній сфері).<br>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.<br>ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів.<br>ПРН 19. Аналізувати та оцінювати захищеність |

| | | |
|---|---|---|
| | | систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення<br>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.<br>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 в кіберпросторі<br>1. Штучний інтелект. Області застосування. Прикладні системи штучного інтелекту<br>2. Інформаційний пошук. Етапи роботи систем інтелектуального аналізу даних. Концепція Data Mining<br>3. Складність алгоритмів. NP-повні задачі. Алгоритми пошуку.<br>4. Теорія ігор. Алгоритми пошуку найкоротшого шляху на карті<br>5. Моделі представлення знань: семантичні мережі, продукційні моделі, фреймові та логіко-лінгвістичні моделі<br>6. Ключові компоненти великих мовних моделей. Основи роботи з ChatGPT та Perplexity: моделі, режими, функції<br>7. Правила побудови, створення та оптимізація промптів.<br>8. Нейромережі. Структура та види нейромереж. Генерування зображень з використанням нейромереж.<br>9. Алгоритми та сервіси генерування аудіо файлів.<br>10. Алгоритми та сервіси генерування відео файлів<br>11. Переваги та недоліки використання технологій штучного інтелекту в кіберпросторі |
| | 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.<br>Рівень підготовки студентів оцінюється наступним чином: |

| | | |
|---|---|---|
| | | “*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок;<br>“*Дуже добре*” (B) – вище середнього рівня з кількома помилками;<br>“*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок;<br>“*Задовільно*” (D) – непогано, але зі значною кількістю недоліків;<br>“*Достатньо*” (E) – виконання задовольняє мінімальні критерії;<br>“*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;<br>“*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 9

Каталог освітнього компонента

| № з/п | Назва складової каталогу | Зміст |
|---|---|---|
| 1. | Галузь знань | 25 Воєнні науки, національна безпека, безпека державного кордону |
| 1.1. | Спеціальність | 256 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:<br>- лекційних занять – 22 год. / 8 год. (заочна);<br>- семінарських занять – 32 год. / 8 год. (заочна);<br>- самостійної роботи – 96 год. / 134 год (заочна) |
| 7. | Програмні результати навчання | ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.<br>ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності.<br>ПРН 5. Розробляти та реалізовувати інноваційні проєкти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів.<br>ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.<br>ПРН 9. Синтезувати спектр заходів та підходів, що можуть використовуватись для вирішення проблем, пов'язаних з викликами глобальній, європейській та регіональній безпеці.<br>ПРН 10. Формувати елементи (складові) стратегії національної безпеки держави (за сферами |

| | | |
|---|---|---|
| | | забезпечення та видами діяльності) (кіберзахист, забезпечення державної безпеки в інформаційній сфері).<br>ПРН 11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання професійних задач у визначених законодавством сферах та за напрямами майбутньої діяльності.<br>ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів.<br>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.<br>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.<br>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.<br>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 1. Концептуальні засади інформаційної безпеки та кібербезпеки<br>Тема 1. Інформаційна складова національної безпеки України<br>Змістовний модуль 2. Інтереси держави в інформаційній сфері<br>Тема 1. Політико-правові аспекти формування інформаційного суспільства держави<br>Тема 2. Інформаційна політика держави<br>Змістовний модуль 3. Загрози безпеці держави в інформаційній сфері<br>Тема 1. Поняття та види загроз безпеці держави в інформаційній сфері<br>Тема 2. Інформаційні загрози людині |

| | | |
|---|---|---|
| | | Змістовний модуль 4. Основи забезпечення інформаційної безпеки<br>Тема 1. Забезпечення інформаційної безпеки держави<br>Змістовний модуль 5. Організаційно-правові засади забезпечення інформаційної безпеки України<br>Тема 1. Система суб'єктів 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.<br>Рівень підготовки студентів оцінюється наступним чином:<br>“*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок;<br>“*Дуже добре*” (B) – вище середнього рівня з кількома помилками;<br>“*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок;<br>“*Задовільно*” (D) – непогано, але зі значною кількістю недоліків;<br>“*Достатньо*” (E) – виконання задовольняє мінімальні критерії;<br>“*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;<br>“*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 | 25 Воєнні науки, національна безпека, безпека державного кордону |
| 1.1. | Спеціальність | 256 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», «Організаційно-правове забезпечення кіберзахисту», «Інформаційне протиборство» |
| 6. | Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах | **5 ЄКТС/ 150 год.**, зокрема для:<br>- лекційних занять – 18 год. / 8 год. (заочна);<br>- семінарських занять – 38 год. / 8 год. (заочна);<br>- 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.<br>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.<br>ПРН 5. Розробляти та реалізовувати інноваційні проєкти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів.<br>ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.<br>ПРН 14. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань |

| | | |
|---|---|---|
| | | національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються.<br>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.<br>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.<br>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) | Змістовний модуль 1. Теоретико-правові засади національної безпеки.<br>Тема 1. Основи теорії національної безпеки. Структура національної безпеки.<br>Тема 2. Структура національної безпеки<br>Тема 3. Загрози і виклики національній безпеці<br>Тема 4. Національні цінності та інтереси<br>Змістовний модуль 2. Україна в сучасному світі.<br>Тема 1. Глобалізація: нові виклики національній безпеці.<br>Тема 2. Геополітика і політична географія сучасного світу.<br>Тема 3. Місце України в сучасному світі.<br>Тема 4. Доктрини національної безпеки провідних країн світу та сусідніх держав, їх вплив на забезпечення національної безпеки України.<br>Змістовний модуль 3. Основні складові національної безпеки.<br>Тема 1. Політична безпека України. Державна безпека України<br>Тема 2. Інформаційна безпека України<br>Тема 3. Воєнна безпека України. Безпека державного кордону<br>Змістовний модуль 4. Служба безпеки України як суб'єкт забезпечення національної безпеки в сфері державної безпеки.<br>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, диференційований залік.<br>Рівень підготовки студентів оцінюється наступним чином:<br>“*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок;<br>“*Дуже добре*” (B) – вище середнього рівня з кількома помилками;<br>“*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок;<br>“*Задовільно*” (D) – непогано, але зі значною кількістю недоліків;<br>“*Достатньо*” (E) – виконання задовольняє мінімальні критерії;<br>“*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;<br>“*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 | 25 Воєнні науки, національна безпека, безпека державного кордону |
| 1.1. | Спеціальність | 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) |
| 1.2. | Рівень вищої освіти | Другий (магістерський) |
| 2. | Назва навчальної дисципліни | **ОК-11. Застосування методів і засобів OSINT у Web-середовищі** |
| 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», «Іноземна мова професійного спрямування», «Теорія прийняття рішень», «Інформаційне протиборство», «Теорія кіберпростору, кібербезпеки та кіберзахисту» |
| 6. | Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах | **4 ЄКТС/ 120 год.**, зокрема для:<br>- лекційних занять – 18 год. / 6 год (заочна);<br>- практичних (лабораторних) занять – 20 год. / 8 год. (заочна);<br>- самостійної роботи – 82 год. / 106 год (заочна) |
| 7. | Програмні результати навчання | ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.<br>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.<br>ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.<br>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.<br>ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення<br>ПРН 21. Досліджувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури |
| 8. | Стислий зміст навчальної дисципліни (назва розділів, тем) | Змістовний модуль 1. Застосування пошукових методів і засобів у WEB-середовищі<br>Тема 1. Web-простір, як середовище пошуку інформації<br>Тема 2. Візуалізація інформації стосовно об'єкту пошуку |
| 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.<br>Рівень підготовки студентів оцінюється наступним чином:<br>"*Відмінно*" (A) – відмінне виконання лише з незначною кількістю помилок;<br>"*Дуже добре*" (B) – вище середнього рівня з кількома помилками;<br>"*Добре*" (C) – у загальному правильна робота з певною кількістю грубих помилок;<br>"*Задовільно*" (D) – непогано, але зі значною кількістю недоліків;<br>"*Достатньо*" (E) – виконання задовольняє мінімальні критерії;<br>"*Незадовільно*" (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;<br>"*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 12

Каталог освітнього компонента

| № з/п | Назва складової каталогу | Зміст |
|---|---|---|
| 1. | Галузь знань | 25 Воєнні науки, національна безпека, безпека державного кордону |
| 1.1. | Спеціальність | 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) |
| 1.2. | Рівень вищої освіти | Другий (магістерський) |
| 2. | Назва навчальної дисципліни | **ОК-12. Методи і моделі протидії кіберзагрозам** |
| 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», «Іноземна мова професійного спрямування», «Теорія прийняття рішень», «Прикладні системи штучного інтелекту в кіберпросторі», «Організаційно-правове забезпечення кіберзахисту» |
| 6. | Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах | **5 ЄКТС/ 150 год.**, зокрема для:<br>- лекційних занять – 18 год. / 8 год. (заочна);<br>- практичних (лабораторних) занять – 38 год. / 8 год (заочна);<br>- самостійної роботи – 94 год. / 134 год. (заочна) |
| 7. | Програмні результати навчання | ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.<br>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.<br>ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.<br>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<br>ПРН 22. Оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації<br>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.<br>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 1. Кіберзагрози. Основні аспекти виявлення та аналізу кіберзагроз<br>1. Поняття та класифікація кіберзагроз. Моделі порушників та їх характеристики<br>2. Методи виявлення та аналізу кіберзагроз<br>3. Класифікація кіберзагроз. Налаштування мережевого моніторингу<br>4. Структура та основні функції систем виявлення вторгнень<br>5. SIEM-системи та їх роль у протидії кіберзагрозам<br>6. Методи кореляції та аналізу подій<br>7. Криптографічні методи протидії кіберзагрозам. Шифрування з симетричним та асиметричним ключем<br>Змістовний модуль 2. Засоби протидії кіберзагрозам<br>1. Методи захисту критичної інформаційної інфраструктури. Приховування даних. Маскування даних. Стеганографія.<br>2. Методи протидії шкідливому програмному забезпеченню<br>3. Моделі захисту від атак соціальної інженерії.<br>4. DLP-системи та методи запобігання витоку даних<br>5. Моделі управління ризиками в кібербезпеці<br>6. Організація захисту кінцевих точок, основні методи. Модель «нульової довіри» Zero Trust.<br>7. Хмарна безпека, методи протидії загрозам у віртуалізованих середовищах<br>8. Моделі кіберзахисту державного рівня. |

| | | |
|---|---|---|
| | | Організаційно-технічна модель кіберзахисту |
| | 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.<br>Рівень підготовки студентів оцінюється наступним чином:<br>“*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок;<br>“*Дуже добре*” (B) – вище середнього рівня з кількома помилками;<br>“*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок;<br>“*Задовільно*” (D) – непогано, але зі значною кількістю недоліків;<br>“*Достатньо*” (E) – виконання задовольняє мінімальні критерії;<br>“*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;<br>“*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 | 25 Воєнні науки, національна безпека, безпека державного кордону |
| 1.1. | Спеціальність | 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) |
| 1.3. | Рівень вищої освіти | Другий (магістерський) |
| 2. | Назва навчальної дисципліни | **ОК-13. 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», «Теорія кіберпростору, кібербезпеки та кіберзахисту», «Прикладні системи штучного інтелекту в кіберпросторі», «Організаційно-правове забезпечення кіберзахисту» |
| 6. | Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах | **6 ЄКТС/ 180 год.**, зокрема для:<br>- лекційних занять – 38 год. / 10 год. (заочна);<br>- практичних (лабораторних) занять – 38 год. / 14 год. (заочна);<br>- самостійної роботи – 104 год. / 156 год. (заочна) |
| 7. | Програмні результати навчання | ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.<br>ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності.<br>ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.<br>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.<br>ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання |

| | | |
|---|---|---|
| | | спеціалізованого програмного забезпечення<br>ПРН 22. Оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації<br>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 1. Технологічні підходи щодо інформаційної безпеки об'єктів критичної інфраструктури<br>1. Вимоги до кіберзахисту об'єктів критичної інфраструктури<br>2. Політика інформаційної безпеки на об'єктах критичної інфраструктури<br>3. Доступ користувачів до об'єктів критичної інфраструктури<br>4. Ідентифікація та автентифікація користувачів об'єкта критичної інфраструктури<br>5. Реєстрація подій та аудит об'єкта критичної інфраструктури<br>Змістовний модуль 2. Мережевий захист компонентів та інформаційних ресурсів об'єктів критичної інформаційної інфраструктури<br>1. Мережевий захист об'єктів критичної інформаційної інфраструктури<br>2. Апаратні та програмні засоби мережевого захисту об'єктів критичної інформаційної інфраструктури<br>3.Аналіз захищеності мережевих об'єктів критичної інфраструктури<br>4. Використання бездротових мереж на об'єктах критичної інфраструктури<br>Змістовний модуль 3. Технологічні та організаційні питання підтримки працездатності інформаційних ресурсів об'єктів критичної інфраструктури<br>1. Забезпечення відмовостійкості об'єктів критичної інфраструктури<br>2. Організаційні та технологічні питання підтримки працездатності інформаційних ресурсів об'єктів критичної інфраструктури<br>Змістовний модуль 4. 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.<br>Рівень підготовки студентів оцінюється наступним чином:<br>“*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок;<br>“*Дуже добре*” (B) – вище середнього рівня з кількома помилками;<br>“*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок;<br>“*Задовільно*” (D) – непогано, але зі значною кількістю недоліків;<br>“*Достатньо*” (E) – виконання задовольняє мінімальні критерії;<br>“*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;<br>“*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 | 25 Воєнні науки, національна безпека, безпека державного кордону |
| 1.1. | Спеціальність | 256 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», «Застосування методів і засобів OSINT у WEB-середовищі», «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:<br>- лекційних занять – 30 год. / 10 год. (заочна);<br>- семінарських занять – 30 год. / 14 год. (заочна);<br>- самостійної роботи – 120 год. / 156 год. (заочна) |
| 7. | Програмні результати навчання | ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.<br>ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності.<br>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.<br>ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.<br>ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових |

| | | |
|---|---|---|
| | | стратегічних підходів.<br>ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.<br>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) | Змістовний модуль 1. Основи управління кіберінцидентами<br>1. Поняття кіберінциденту та події інформаційної безпеки. Найвідоміші кіберінциденти в Україні та світі<br>2. Категоризація та життєвий цикл кіберінцидентів.<br>3. Джерела даних, методи та засоби виявлення кіберінцидентів<br>4. Виявлення подій. Знайомство з платформою MISP<br>5. Класифікація вразливостей комп'ютерних мереж та систем<br>6. Сортування та аналіз подій<br>7. Реагування та відновлення після кіберінциденту<br>8. Поліпшення можливостей в процесі управління подіями інформаційної безпеки. Ретроспектива<br>Змістовний модуль 2. Реагування на кіберінциденти<br>1. Класифікація вразливостей інформаційних систем<br>2. Моніторинг подій інформаційної безпеки<br>3. Центри операційної безпеки, їх основні функції, структура та ролі. Команди реагування на кіберінциденти SERT/CSIRT, їх відмінності<br>4. Засоби реагування на кіберінциденти. Рішення для захисту кінцевих точок EDR/XDR, SIEM/SOAR/xSOAR<br>5. Аналіз інцидентів та цифрова криміналістика. Цифрові докази<br>6. Організаційні та правові аспекти розслідування кіберінцидентів<br>7. Національне та міжнародне законодавство у сфері кібербезпеки. Звітування та комунікація |
| 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.<br>Рівень підготовки студентів оцінюється наступним чином:<br>“*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок;<br>“*Дуже добре*” (B) – вище середнього рівня з кількома помилками;<br>“*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок;<br>“*Задовільно*” (D) – непогано, але зі значною кількістю недоліків;<br>“*Достатньо*” (E) – виконання задовольняє мінімальні критерії;<br>“*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;<br>“*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 | 25 Воєнні науки, національна безпека, безпека державного кордону |
| 1.1. | Спеціальність | 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) |
| 1.2. | Рівень вищої освіти | Другий (магістерський) |
| 2. | Назва навчальної дисципліни | **ОК-15. 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», «Застосування методів і засобів OSINT у Web-середовищі», «Методи і моделі протидії кіберзагрозам», «Кіберзахист об'єктів критичної інфраструктури» |
| 6. | Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах | **5 ЄКТС/ 150 год.**, зокрема для:<br>- лекційних занять – 30 год. / 8 год (заочна);<br>- семінарських занять – 30 год. / 8 год. (заочна);<br>- самостійної роботи – 60 год. / 134 год. (заочна) |
| 7. | Програмні результати навчання | ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.<br>ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності.<br>ПРН 4. Організовувати роботу колективу, забезпечувати професійний розвиток його членів та досягнення поставлених цілей.<br>ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.<br>ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів.<br>ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, |

| | | |
|---|---|---|
| | | технології створення та використання спеціалізованого програмного забезпечення<br>ПРН 21. Досліджувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури<br>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. Основи аудиту інформаційної безпеки та кібербезпеки<br>1. Вступ до аудиту інформаційної безпеки та кібербезпеки: поняття, цілі, види<br>2. Кращі світові практики, стандарти і вимоги до проведення процедур аудиту інформаційної безпеки та кібербезпеки<br>3. Ризик-орієнтований підхід в аудиті інформаційної безпеки та кібербезпеки.<br>4. Аналіз політики інформаційної безпеки за стандартом ISO/IEC 27001, 27002, 27004<br>5. Правові аспекти аудиту інформаційної безпеки та кібербезпеки<br>6. Методологія та етапи проведення аудиту інформаційної безпеки та кібербезпеки<br>7. Методи та заходи планування процедур моніторингу операційних процесів установи<br>8. Аудит фізичної безпеки інформаційних систем, аудит управління доступом та аудит захисту від шкідливого програмного забезпечення.<br>9. Аудит безпеки систем промислової автоматизації (SCADA)<br>Змістовний модуль 2. Організація проведення аудиту інформаційної безпеки та кібербезпеки<br>1. Організація процесу аудиту інформаційної безпеки та кібербезпеки. Ініціювання процедури аудиту<br>2. Послідовність дій та етапів аудиту інформаційної безпеки та кібербезпеки. Збір інформації для проведення аудиту та аналіз даних під час аудиту<br>3. Аналіз результатів аудиту та системи кібербезпеки.<br>4. Формування звітності на основі проведення аудиту інформаційної безпеки та кібербезпеки: документування результатів аудиту та підготовка аудиторського звіту<br>5. Концепція впровадження системи аудиту |

| | | |
|---|---|---|
| | | інформаційної безпеки в Україні (“Дорожня карта”)<br>6. Етапи реалізації Дорожньої карти створення системи контролю та аудиту інформаційної безпеки та кібербезпеки в Україні |
| 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.<br>Рівень підготовки студентів оцінюється наступним чином:<br>“*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок;<br>“*Дуже добре*” (B) – вище середнього рівня з кількома помилками;<br>“*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок;<br>“*Задовільно*” (D) – непогано, але зі значною кількістю недоліків;<br>“*Достатньо*” (E) – виконання задовольняє мінімальні критерії;<br>“*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;<br>“*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 | 25 Воєнні науки, національна безпека, безпека державного кордону |
| 1.1. | Спеціальність | 256 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», «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:<br>- лекційних занять – 20 год. / 6 год (заочна);<br>- семінарських занять – 20 год. / 8 год. практичних (заочна);<br>- самостійної роботи – 80 год. / 106 год (заочна) |
| 7. | Програмні результати навчання | ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.<br>ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.<br>ПРН 9. Синтезувати спектр заходів та підходів, що можуть використовуватись для вирішення проблем, пов'язаних з викликами глобальній, європейській та регіональній безпеці.<br>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.<br>ПРН 21. Досліджувати системи та засоби |

| | | |
|---|---|---|
| | | інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури<br>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.<br>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 технології<br>Тема 1. Розподілені обчислювальні системи та основи хмарних обчислень.<br>Тема 2. Технологічні основи хмарних технологій.<br>Тема 3. Захист інформації під час використання хмарних сервісів<br>Тема 4. Протидія загрозам у сфері розподілених систем |
| | Запланована навчальна діяльність та методи навчання | Навчальна діяльність здійснюється шляхом лекційних, семінарських (для заочної форми 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.<br>Рівень підготовки студентів оцінюється наступним чином:<br>"*Відмінно*" (A) – відмінне виконання лише з незначною кількістю помилок;<br>"*Дуже добре*" (B) – вище середнього рівня з кількома помилками;<br>"*Добре*" (C) – у загальному правильна робота з певною кількістю грубих помилок;<br>"*Задовільно*" (D) – непогано, але зі значною кількістю недоліків;<br>"*Достатньо*" (E) – виконання задовольняє мінімальні критерії;<br>"*Незадовільно*" (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;<br>"*Незадовільно*" (F) – необхідна серйозна подальша робота. |
| 11. | Мова навчання | Українська |

| | | |
|---|---|---|
| | (українська та/або іноземні мови) | |
| 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 | 25 Воєнні науки, національна безпека, безпека державного кордону |
| 1.1. | Спеціальність | 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) |
| 1.3. | Рівень вищої освіти | Другий (магістерський) |
| 2. | Назва навчальної дисципліни | **ОК-17. Територіальна оборона, мобілізаційна підготовка та мобілізація** |
| 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» |
| 6. | Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах | **4 ЄКТС/ 120 год.**, зокрема для:<br>- лекційних занять – 30 год. / 8 год. (заочна);<br>- семінарських занять – 30 год. / 6 год (заочна);<br>- 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.<br>ПРН 10. Формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності) (кіберзахист, забезпечення державної безпеки в інформаційній сфері).<br>ПРН 13. Організовувати та здійснювати керівництво територіальною обороною, мобілізаційною підготовкою та мобілізацією у межах професійної компетентності.<br>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 1. Теоретичні основи та елементи національного спротиву в Україні<br>Тема 1. Особливості сучасного безпекового середовища України: роль і місце національного спротиву. Кіберрезерв сил територіальної оборони та руху опору України.<br>Тема 2. Взаємодія і співпраця сил безпеки та оборони у системі національного спротиву. Структурно-функціональна модель організації територіальної оборони в Україні.<br>Тема 3. Підготовка громадян України до національного спротиву. Кіберрезерв сил територіальної оборони.<br>Модуль 2. Основи мобілізаційної підготовки та мобілізації в Україні.<br>Тема 1. Основні принципи, зміст та організаційно-правові основи проведення мобілізаційної підготовки та мобілізації.<br>Тема 2. Обов'язки підприємств, установ і організацій та громадян щодо мобілізаційної підготовки та мобілізації.<br>Тема 3. Структура, зміст та порядок оформлення оперативно-мобілізаційних документів. Виконання мобілізаційних планів, завдань (замовлень) в умовах правового режиму воєнного стану. |
| 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.<br>Рівень підготовки студентів оцінюється наступним чином:<br>"*Відмінно*" (A) – відмінне виконання лише з незначною кількістю помилок;<br>"*Дуже добре*" (B) – вище середнього рівня з кількома помилками;<br>"*Добре*" (C) – у загальному правильна робота з певною кількістю грубих помилок;<br>"*Задовільно*" (D) – непогано, але зі значною |

| | | |
|---|---|---|
| | | кількістю недоліків;<br>“*Достатньо*” (E) – виконання задовольняє мінімальні критерії;<br>“*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;<br>“*Незадовільно*” (F) – необхідна серйозна подальша робота. |
| 11. | Мова навчання (українська та/або іноземні мови) | Українська |
| 12. | Додаткова інформація (у разі потреби) | Немає |

Спеціальна кафедра 2 «Боротьба з тероризмом» центру захисту національної державності Навчально-наукового інституту державної безпеки

Додаток 18

Каталог освітнього компонента

| № з/п | Назва складової каталогу | Зміст |
|---|---|---|
| 1. | Галузь знань | 25 Воєнні науки, національна безпека, безпека державного кордону |
| 1.1. | Спеціальність | 256 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», «Іноземна мова професійного спрямування», «Гендерна політика в секторі безпеки та оборони України», «Теорія кіберпростору, кібербезпеки та кіберзахисту», «Інформаційне протиборство», «Прикладні системи штучного інтелекту в кіберпросторі», «Організаційно-правове забезпечення кіберзахисту», «Актуальні проблеми інформаційної безпеки», «Застосування методів і засобів OSINT у WEB-середовищі», «Методи і моделі протидії кіберзагрозам», «Кіберзахист об'єктів критичної інфраструктури», «Управління кіберінцидентами», «Аудит інформаційної безпеки та кібербезпеки», «Безпека розподілених інформаційних ресурсів та хмарні технології», «Територіальна оборона, мобілізаційна підготовка та мобілізація» |
| 6. | Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах | **9 ЄКТС/ 270 год.**, зокрема для:<br>- самостійної роботи – 270 год. |
| 7. | Програмні результати навчання | ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.<br>ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності.<br>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.<br>ПРН 4. Організовувати роботу колективу, забезпечувати професійний розвиток його членів та досягнення поставлених цілей.<br>ПРН 5. Розробляти та реалізовувати інноваційні проєкти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів.<br>ПРН 6. Вільно спілкуватися державною та іноземною мовами усно і письмово для обговорення професійної діяльності, результатів досліджень та інновацій, пошуку та аналізу відповідної інформації.<br>ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.<br>ПРН 9. Синтезувати спектр заходів та підходів, що можуть використовуватись для вирішення проблем, пов'язаних з викликами глобальній, європейській та регіональній безпеці.<br>ПРН 10. Формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності) (кіберзахист, забезпечення державної безпеки в інформаційній сфері).<br>ПРН 11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання професійних задач у визначених законодавством сферах та за напрямами майбутньої діяльності.<br>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.<br>ПРН 13. Організовувати та здійснювати керівництво територіальною обороною, мобілізаційною підготовкою та мобілізацією у межах професійної компетентності.<br>ПРН 14. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються.<br>ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів.<br>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.<br>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.<br>ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення<br>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.<br>ПРН 21. Досліджувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури<br>ПРН 22. Оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації<br>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.<br>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.<br>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 | Змістовний модуль 1. Науково-дослідна практика<br>Тема 1. Розробка індивідуального графіку |

| | | |
|---|---|---|
| | розділів, тем) | проходження практики. Узгодження його з науковим керівником кваліфікаційної (магістерської) роботи та керівником практики від кафедри.<br>Тема 2. Визначення предмету та об'єкту дослідження, мети та завдань дослідження відповідно до закріпленої за здобувачем теми кваліфікаційної (магістерської) роботи<br>Тема 3. Ознайомлення з науковими напрямами роботи на базі практики<br>Тема 4. Ознайомлення з іноземними та вітчизняними науково-інформаційними джерелами за спеціалізацією, обрання наукової проблематики та формування бібліографії<br>Тема 5. Збір та обробка даних щодо стану об'єкту дослідження на базі практики.<br>Тема 6. Ознайомлення з нормативно-правовою документацією за обраною проблематикою та формування напрямів удосконалення стану об'єкту дослідження.<br>Тема 7. Виконання індивідуального завдання відповідно до теми кваліфікаційної (магістерської) роботи<br>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.<br>Рівень підготовки студентів оцінюється наступним чином:<br>"*Відмінно*" (A) – відмінне виконання лише з незначною кількістю помилок;<br>"*Дуже добре*" (B) – вище середнього рівня з кількома помилками;<br>"*Добре*" (C) – у загальному правильна робота з певною кількістю грубих помилок;<br>"*Задовільно*" (D) – непогано, але зі значною кількістю недоліків;<br>"*Достатньо*" (E) – виконання задовольняє мінімальні критерії;<br>"*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 | 25 Воєнні науки, національна безпека, безпека державного кордону |
| 1.1. | Спеціальність | 256 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», «Іноземна мова професійного спрямування», «Гендерна політика в секторі безпеки та оборони України», «Теорія кіберпростору, кібербезпеки та кіберзахисту», «Інформаційне протиборство», «Прикладні системи штучного інтелекту в кіберпросторі», «Організаційно-правове забезпечення кіберзахисту», «Актуальні проблеми інформаційної безпеки», «Застосування методів і засобів OSINT у WEB-середовищі», «Методи і моделі протидії кіберзагрозам», «Кіберзахист об'єктів критичної інфраструктури», «Управління кіберінцидентами», «Аудит інформаційної безпеки та кібербезпеки», «Безпека розподілених інформаційних ресурсів та хмарні технології», «Територіальна оборона, мобілізаційна підготовка та мобілізація», «Науково-дослідна практика» |
| 6. | Обсяг навчальної дисципліни в кредитах ЄКТС, що присвоюються, та годинах | **6 ЄКТС/180 год.**, зокрема для:<br>- самостійної роботи – 180 год. |
| 7. | Програмні результати навчання | ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.<br>ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності.<br>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.<br>ПРН 4. Організовувати роботу колективу, забезпечувати професійний розвиток його членів та досягнення поставлених цілей.<br>ПРН 5. Розробляти та реалізовувати інноваційні проєкти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів.<br>ПРН 6. Вільно спілкуватися державною та іноземною мовами усно і письмово для обговорення професійної діяльності, результатів досліджень та інновацій, пошуку та аналізу відповідної інформації.<br>ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.<br>ПРН 9. Синтезувати спектр заходів та підходів, що можуть використовуватись для вирішення проблем, пов'язаних з викликами глобальній, європейській та регіональній безпеці.<br>ПРН 10. Формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності) (кіберзахист, забезпечення державної безпеки в інформаційній сфері).<br>ПРН 11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання професійних задач у визначених законодавством сферах та за напрямами майбутньої діяльності.<br>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.<br>ПРН 13. Організовувати та здійснювати керівництво територіальною обороною, мобілізаційною підготовкою та мобілізацією у межах професійної компетентності.<br>ПРН 14. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються.<br>ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів.<br>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.<br>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.<br>ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення<br>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.<br>ПРН 21. Досліджувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури<br>ПРН 22. Оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації<br>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.<br>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.<br>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 | Теми кваліфікаційних (магістерських) робіт затверджуються Наказом Національної академії |

| | | |
|---|---|---|
| | розділів, тем) | 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.<br>Рівень підготовки студентів оцінюється наступним чином:<br>“*Відмінно*” (A) – відмінне виконання лише з незначною кількістю помилок;<br>“*Дуже добре*” (B) – вище середнього рівня з кількома помилками;<br>“*Добре*” (C) – у загальному правильна робота з певною кількістю грубих помилок;<br>“*Задовільно*” (D) – непогано, але зі значною кількістю недоліків;<br>“*Достатньо*” (E) – виконання задовольняє мінімальні критерії;<br>“*Незадовільно*” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;<br>“*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