

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: <ul style="list-style-type: none"> - лекційних занять – 12 год. / 8 год. (заочна); - семінарських занять – 10 год. / 4 год. (заочна); - практичних (лабораторних) занять – 10 год. / 2 год. (заочна); - самостійної роботи – 58 год. / 76 год (заочна).
7.	Програмні результати навчання	<p>ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.</p> <p>ПРН 5. Розробляти та реалізовувати інноваційні проекти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів.</p> <p>ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.</p> <p>ПРН 11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання професійних задач у визначених законодавством сферах та за напрямками майбутньої діяльності.</p> <p>ПРН 14. Зрозуміло і недвозначно доносити власні</p>

		<p>знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються.</p> <p>ПРН 17. Створювати та документально оформлювати організаційно-технічні та організаційно-правові моделі кіберзахисту, а також моделі захисту конфіденційності, організувати 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.</p>
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	<p>Змістовний модуль 1. Основи організації та методологія наукових досліджень.</p> <p>Тема 1. Система організації та управління науковими дослідженнями в Україні. Академічна доброчесність</p> <p>Тема 2. Методологія наукових досліджень та її значення у науковій роботі.</p> <p>Тема 3. Загальнонаукові методи дослідження / Градація методів наукового дослідження (заочна)</p> <p>Змістовний модуль 2. Теорія та практика наукових досліджень.</p> <p>Тема 1. Основи когнітивної творчості дослідника / Магістерська праця: характеристика, етапи проведення, сучасні вимоги (заочна)</p> <p>Тема 2. Підготовка публікацій, доповідей і повідомлень на наукових заходах.</p> <p>Тема 3. Оформлення і захист результатів дослідження.</p>
9.	Запланована навчальна діяльність та методи навчання	<p>Навчальна діяльність здійснюється шляхом лекційних, семінарських, практичних занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій.</p>
10.	Методи і критерії оцінювання	<p>Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, диференційований залік.</p> <p>Рівень підготовки студентів оцінюється наступним чином:</p> <p>“Відмінно” (A) – відмінне виконання лише з незначною кількістю помилок;</p> <p>“Дуже добре” (B) – вище середнього рівня з кількома помилками;</p> <p>“Добре” (C) – у загальному правильна робота з певною кількістю грубих помилок;</p> <p>“Задовільно” (D) – непогано, але зі значною кількістю недоліків;</p> <p>“Достатньо” (E) – виконання задовольняє мінімальні критерії;</p> <p>“Незадовільно” (FX) – потрібно працювати перед</p>

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

Кафедра філософії
Навчально-наукового гуманітарного інституту

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: <ul style="list-style-type: none"> - лекційних занять – 12 год. / 8 год. (заочна); - семінарських занять – 20 год. / 6 год. (заочна); - самостійної роботи – 58 год. / 76 год (заочна).
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 6. Вільно спілкуватися державною та іноземною мовами усно і письмово для обговорення професійної діяльності, результатів досліджень та інновацій, пошуку та аналізу відповідної інформації. ПРН 14. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Модуль І. Державна мова в науковій комунікації професіонала з організації інформаційної безпеки 1. Специфіка наукового тексту й професійного наукового викладу думки 2. Морфологічні норми фахового наукового мовлення професіонала з організації

		інформаційної безпеки 3. Синтаксичні норми фахового наукового мовлення професіонала з організації інформаційної безпеки 4. Укладання фахового публічного виступу професіонала з організації інформаційної безпеки 5. Мистецтво виголошення фахового публічного виступу професіонала з організації інформаційної безпеки. Мовна поведінка оратора. 6. Культура писемного наукового мовлення професіонала з організації інформаційної безпеки
9.	Запланована навчальна діяльність та методи навчання	Навчальна діяльність здійснюється шляхом лекційних, семінарських занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій.
10.	Методи і критерії оцінювання	Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, диференційований залік. Рівень підготовки студентів оцінюється наступним чином: “Відмінно” (A) – відмінне виконання лише з незначною кількістю помилок; “Дуже добре” (B) – вище середнього рівня з кількома помилками; “Добре” (C) – у загальному правильна робота з певною кількістю грубих помилок; “Задовільно” (D) – непогано, але зі значною кількістю недоліків; “Достатньо” (E) – виконання задовольняє мінімальні критерії; “Незадовільно” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку; “Незадовільно” (F) – необхідна серйозна подальша робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра української ділової мови
Навчально-наукового гуманітарного інституту

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: <ul style="list-style-type: none"> - лекційних занять – 12 год. / 8 год. (заочна); - семінарських занять – 10 год. / 4 год. (заочна); - практичних (лабораторних) занять – 10 год. / 2 год. (заочна); - самостійної роботи – 58 год. / 76 год (заочна).
7.	Програмні результати навчання	<p>ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.</p> <p>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.</p> <p>ПРН 4. Організувати роботу колективу, забезпечувати професійний розвиток його членів та досягнення поставлених цілей.</p> <p>ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.</p> <p>ПРН 11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання</p>

		<p>професійних задач у визначених законодавством сферах та за напрямками майбутньої діяльності.</p> <p>ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів.</p> <p>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.</p> <p>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.</p>
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	<p>Модуль I. Основи теорії прийняття рішень</p> <p>Тема 1.1. Основи теорії прийняття рішень.</p> <p>Тема 1.2. Невизначеності в теорії прийняття рішень</p> <p>Модуль II. Методи та моделі в теорії прийняття рішень</p> <p>Тема 2.1. Методи прийняття рішень</p> <p>Тема 2.2. Моделювання в теорії прийняття рішень</p>
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	<p>Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, диференційований залік.</p> <p>Рівень підготовки студентів оцінюється наступним чином:</p> <p>“Відмінно” (A) – відмінне виконання лише з незначною кількістю помилок;</p> <p>“Дуже добре” (B) – вище середнього рівня з кількома помилками;</p> <p>“Добре” (C) – у загальному правильна робота з певною кількістю грубих помилок;</p> <p>“Задовільно” (D) – непогано, але зі значною кількістю недоліків;</p> <p>“Достатньо” (E) – виконання задовольняє мінімальні критерії;</p> <p>“Незадовільно” (FX) – потрібно працювати перед</p>

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

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: <ul style="list-style-type: none"> - практичних (лабораторних) занять – 88 год. / 24 год (заочна); - самостійної роботи – 92 год. / 156 год (заочна).
7.	Програмні результати навчання	ПРН 5. Розробляти та реалізовувати інноваційні проекти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів. ПРН 6. Вільно спілкуватися державною та іноземною мовами усно і письмово для обговорення професійної діяльності, результатів досліджень та інновацій, пошуку та аналізу відповідної інформації. ПРН 14. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Модуль I. Робота з джерелами інформації. Тема 1. Типи інформаційних джерел. Тема 2. Аналіз наукової літератури професійного спрямування. Тема 3. Типи інформації. Основні характеристики.

		<p>Модуль II. Інформаційна безпека. Тема 1. Основні засади інформаційної безпеки. Тема 2. Основні загрози інформаційній безпеці. Тема 3. Захист інформації, методи і способи протидії основним загрозам.</p> <p>Модуль III. Стратегії успішного працевлаштуванні. Тема 1. Підготовка необхідних форм документації для успішного працевлаштування. Тема 2. Співбесіда як вирішальний етап працевлаштування.</p>
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	<p>Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, диференційований залік та екзамен.</p> <p>Рівень підготовки студентів оцінюється наступним чином: <i>“Відмінно”</i> (A) – відмінне виконання лише з незначною кількістю помилок; <i>“Дуже добре”</i> (B) – вище середнього рівня з кількома помилками; <i>“Добре”</i> (C) – у загальному правильна робота з певною кількістю грубих помилок; <i>“Задовільно”</i> (D) – непогано, але зі значною кількістю недоліків; <i>“Достатньо”</i> (E) – виконання задовольняє мінімальні критерії; <i>“Незадовільно”</i> (FX) – потрібно працювати перед тим, як отримати позитивну оцінку; <i>“Незадовільно”</i> (F) – необхідна серйозна подальша робота.</p>
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

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: <ul style="list-style-type: none"> - лекційних занять – 10 год. / 6 год (заочна); - семінарських занять – 20 год. / 6 год (заочна); - самостійної роботи – 60 год. / 78 год (заочна)
7.	Програмні результати навчання	ПРН 4. Організувати роботу колективу, забезпечувати професійний розвиток його членів та досягнення поставлених цілей. ПРН 8. Забезпечувати дотримання принципу гендерної рівності під час здійснення професійної діяльності. ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Модуль І. Теоретично-правові та практичні питання забезпечення гендерної рівності в секторі безпеки і оборони. Тема 1. Поняття гендер, гендерна рівність, гендерна чутливість у суспільно-політичному та науковому дискурсах. Міжнародно-правове забезпечення гендерної рівності. Українське законодавство щодо гендерних питань Тема 2. Гендерно чутливі комунікації в секторі безпеки і оборони. Передумова, наслідки і протидія

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

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

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: <ul style="list-style-type: none"> - лекційних занять – 22 год. / 6 год. (заочна); - семінарських занять – 22 год. / 8 год. (заочна); - самостійної роботи – 76 год. / 106 год (заочна)
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН 10. Формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності) (кіберзахист, забезпечення державної безпеки в інформаційній сфері). ПРН 16. Організувати та спрямовувати діяльність фахівців з кіберзахисту у сфері інформаційних технологій та кіберпросторі; розробляти та впроваджувати заходи із кіберзахисту у сфері інформаційних технологій та кіберпросторі, самостійно та у взаємодії з контролюючими органами. ПРН 17. Створювати та документально

		<p>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.</p> <p>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.</p>
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	<p>Змістовний модуль 1. Основи теорії кіберпростору.</p> <p>Тема 1. Основні положення та визначення кіберпростору.</p> <p>Тема 2. Основні напрями розвитку теорії кіберпростору.</p> <p>Тема 3. Основи спілкування у кіберпросторі.</p> <p>Тема 4. Основи економіки кіберпростору.</p> <p>Тема 5. Основні напрями розвитку гуманітарних наук у кіберпросторі.</p> <p>Модуль 2. Основи кібербезпеки</p> <p>Тема 6. Основні напрями розвитку теорії і практики кібербезпеки у контексті забезпечення національної безпеки та безпеки держави.</p> <p>Тема 7. Основні підходи до визначення видів протиборства в інформаційній сфері та кіберпросторі.</p> <p>Тема 8. Війна як один із способів протиборства в інформаційній сфері та кіберпросторі.</p> <p>Тема 9. Основи теорії і практики щодо розробки технології забезпечення кібербезпеки</p> <p>Модуль 3. Основи кіберзахисту</p> <p>Тема 10. Теоретичні основи щодо створення архітектури захисту кіберпростору.</p>
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	<p>Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, екзамен.</p> <p>Рівень підготовки студентів оцінюється наступним чином:</p> <p>“Відмінно” (А) – відмінне виконання лише з незначною кількістю помилок;</p> <p>“Дуже добре” (В) – вище середнього рівня з кількома помилками;</p>

		<p>“Добре” (С) – у загальному правильна робота з певною кількістю грубих помилок;</p> <p>“Задовільно” (D) – непогано, але зі значною кількістю недоліків;</p> <p>“Достатньо” (E) – виконання задовольняє мінімальні критерії;</p> <p>“Незадовільно” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;</p> <p>“Незадовільно” (F) – необхідна серйозна подальша робота.</p>
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

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: <ul style="list-style-type: none"> - лекційних занять – 22 год. / 8 год. (заочне); - семінарських занять – 32 год. / 8 год. (заочне); - самостійної роботи – 96 год. / 134 год. (заочне)
7.	Програмні результати навчання	<p>ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності.</p> <p>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.</p> <p>ПРН 5. Розробляти та реалізовувати інноваційні проекти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів.</p> <p>ПРН 8. Забезпечувати дотримання принципу гендерної рівності під час здійснення професійної діяльності.</p> <p>ПРН 11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання</p>

		<p>професійних задач у визначених законодавством сферах та за напрямками майбутньої діяльності.</p> <p>ПРН 13. Організувати та здійснювати керівництво територіальною обороною, мобілізаційною підготовкою та мобілізацією у межах професійної компетентності.</p> <p>ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів.</p> <p>ПРН 16. Організувати 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.</p> <p>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.</p> <p>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.</p>
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	<p>Змістовий модуль I. Інформаційне протиборство як механізм забезпечення національної безпеки в інформаційній сфері</p> <p>Тема 1. Генезис інформаційного протиборства</p> <p>Тема 2. Сучасні стратегії та концепції інформаційного протиборства</p> <p>Змістовий модуль II. Теоретичні та технологічні основи інформаційного протиборства</p> <p>Тема 3. Теоретичні основи інформаційного протиборства</p> <p>Тема 4. Технології та засоби інформаційного протиборства</p> <p>Змістовий модуль III. Організаційні аспекти підготовки та ведення інформаційного протиборства</p> <p>Тема 5. Форми ведення інформаційного протиборства</p> <p>Тема 6. Підготовка та ведення інформаційного протиборства з використанням соціально-орієнтованих ресурсів мережі Internet та відкритих даних</p> <p>Тема 7. Перспективи ведення інформаційного</p>

		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	<p>Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, екзамен.</p> <p>Рівень підготовки студентів оцінюється наступним чином:</p> <p>“Відмінно” (A) – відмінне виконання лише з незначною кількістю помилок;</p> <p>“Дуже добре” (B) – вище середнього рівня з кількома помилками;</p> <p>“Добре” (C) – у загальному правильна робота з певною кількістю грубих помилок;</p> <p>“Задовільно” (D) – непогано, але зі значною кількістю недоліків;</p> <p>“Достатньо” (E) – виконання задовольняє мінімальні критерії;</p> <p>“Незадовільно” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;</p> <p>“Незадовільно” (F) – необхідна серйозна подальша робота.</p>
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

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: <ul style="list-style-type: none"> - лекційних занять – 22 год. / 6 год. (заочна); - практичних (лабораторних) занять – 22 год. / 8 год. (заочна); - самостійної роботи – 76 год. / 106 год. (заочна)
7.	Програмні результати навчання	<p>ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.</p> <p>ПРН 10. Формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності) (кіберзахист, забезпечення державної безпеки в інформаційній сфері).</p> <p>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.</p> <p>ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів.</p> <p>ПРН 19. Аналізувати та оцінювати захищеність</p>

		<p>систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення</p> <p>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.</p> <p>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.</p>
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	<p>Модуль І. Прикладні системи штучного інтелекту в кіберпросторі</p> <ol style="list-style-type: none"> 1. Штучний інтелект. Области застосування. Прикладні системи штучного інтелекту 2. Інформаційний пошук. Етапи роботи систем інтелектуального аналізу даних. Концепція Data Mining 3. Складність алгоритмів. NP-повні задачі. Алгоритми пошуку. 4. Теорія ігор. Алгоритми пошуку найкоротшого шляху на карті 5. Моделі представлення знань: семантичні мережі, продукційні моделі, фреймові та логіко-лінгвістичні моделі 6. Ключові компоненти великих мовних моделей. Основи роботи з ChatGPT та Perplexity: моделі, режими, функції 7. Правила побудови, створення та оптимізація промптів. 8. Нейромережі. Структура та види нейромереж. Генерування зображень з використанням нейромереж. 9. Алгоритми та сервіси генерування аудіо файлів. 10. Алгоритми та сервіси генерування відео файлів 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	<p>Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, диференційований залік.</p> <p>Рівень підготовки студентів оцінюється наступним чином:</p>

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

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: - лекційних занять – 22 год. / 8 год. (заочна); - семінарських занять – 32 год. / 8 год. (заочна); - самостійної роботи – 96 год. / 134 год (заочна)
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності. ПРН 5. Розробляти та реалізовувати інноваційні проекти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів. ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН 9. Синтезувати спектр заходів та підходів, що можуть використовуватись для вирішення проблем, пов'язаних з викликами глобальній, європейській та регіональній безпеці. ПРН 10. Формувати елементи (складові) стратегії національної безпеки держави (за сферами

		<p>забезпечення та видами діяльності) (кіберзахист, забезпечення державної безпеки в інформаційній сфері).</p> <p>ПРН 11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання професійних задач у визначених законодавством сферах та за напрямками майбутньої діяльності.</p> <p>ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів.</p> <p>ПРН 17. Створювати та документально оформлювати організаційно-технічні та організаційно-правові моделі кіберзахисту, а також моделі захисту конфіденційності, організувати 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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	<p>Змістовний модуль 1. Концептуальні засади інформаційної безпеки та кібербезпеки</p> <p>Тема 1. Інформаційна складова національної безпеки України</p> <p>Змістовний модуль 2. Інтереси держави в інформаційній сфері</p> <p>Тема 1. Політико-правові аспекти формування інформаційного суспільства держави</p> <p>Тема 2. Інформаційна політика держави</p> <p>Змістовний модуль 3. Загрози безпеці держави в інформаційній сфері</p> <p>Тема 1. Поняття та види загроз безпеці держави в інформаційній сфері</p> <p>Тема 2. Інформаційні загрози людині</p>

		<p>Змістовний модуль 4. Основи забезпечення інформаційної безпеки</p> <p>Тема 1. Забезпечення інформаційної безпеки держави</p> <p>Змістовний модуль 5. Організаційно-правові засади забезпечення інформаційної безпеки України</p> <p>Тема 1. Система суб'єктів забезпечення інформаційної безпеки України</p>
	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	<p>Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, екзамен.</p> <p>Рівень підготовки студентів оцінюється наступним чином:</p> <p>“Відмінно” (А) – відмінне виконання лише з незначною кількістю помилок;</p> <p>“Дуже добре” (В) – вище середнього рівня з кількома помилками;</p> <p>“Добре” (С) – у загальному правильна робота з певною кількістю грубих помилок;</p> <p>“Задовільно” (D) – непогано, але зі значною кількістю недоліків;</p> <p>“Достатньо” (Е) – виконання задовольняє мінімальні критерії;</p> <p>“Незадовільно” (FХ) – потрібно працювати перед тим, як отримати позитивну оцінку;</p> <p>“Незадовільно” (F) – необхідна серйозна подальша робота.</p>
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

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: <ul style="list-style-type: none"> - лекційних занять – 18 год. / 8 год. (заочна); - семінарських занять – 38 год. / 8 год. (заочна); - самостійної роботи – 94 год. / 134 год. (заочна)
7.	Програмні результати навчання	<p>ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності.</p> <p>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.</p> <p>ПРН 5. Розробляти та реалізовувати інноваційні проекти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів.</p> <p>ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.</p> <p>ПРН 14. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань</p>

		<p>національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються.</p> <p>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.</p> <p>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.</p> <p>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.</p>
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	<p>Змістовний модуль 1. Теоретико-правові засади національної безпеки.</p> <p>Тема 1. Основи теорії національної безпеки. Структура національної безпеки.</p> <p>Тема 2. Структура національної безпеки</p> <p>Тема 3. Загрози і виклики національній безпеці</p> <p>Тема 4. Національні цінності та інтереси</p> <p>Змістовний модуль 2. Україна в сучасному світі.</p> <p>Тема 1. Глобалізація: нові виклики національній безпеці.</p> <p>Тема 2. Геополітика і політична географія сучасного світу.</p> <p>Тема 3. Місце України в сучасному світі.</p> <p>Тема 4. Доктрини національної безпеки провідних країн світу та сусідніх держав, їх вплив на забезпечення національної безпеки України.</p> <p>Змістовний модуль 3. Основні складові національної безпеки.</p> <p>Тема 1. Політична безпека України. Державна безпека України</p> <p>Тема 2. Інформаційна безпека України</p> <p>Тема 3. Воєнна безпека України. Безпека державного кордону</p> <p>Змістовний модуль 4. Служба безпеки України як суб'єкт забезпечення національної безпеки в сфері державної безпеки.</p> <p>Тема 1. Організаційно-правові засади протидії Службою безпеки України основним реальним та потенційним загрозам і викликам національній безпеці та національним інтересам України у</p>

		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	<p>Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, диференційований залік.</p> <p>Рівень підготовки студентів оцінюється наступним чином:</p> <p>“Відмінно” (А) – відмінне виконання лише з незначною кількістю помилок;</p> <p>“Дуже добре” (В) – вище середнього рівня з кількома помилками;</p> <p>“Добре” (С) – у загальному правильна робота з певною кількістю грубих помилок;</p> <p>“Задовільно” (D) – непогано, але зі значною кількістю недоліків;</p> <p>“Достатньо” (Е) – виконання задовольняє мінімальні критерії;</p> <p>“Незадовільно” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;</p> <p>“Незадовільно” (F) – необхідна серйозна подальша робота.</p>
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

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: <ul style="list-style-type: none"> - лекційних занять – 18 год. / 6 год (заочна); - практичних (лабораторних) занять – 20 год. / 8 год. (заочна); - самостійної роботи – 82 год. / 106 год (заочна)
7.	Програмні результати навчання	<p>ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.</p> <p>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.</p> <p>ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.</p> <p>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</p>

		забезпечення. ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення ПРН 21. Досліджувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Змістовний модуль 1. Застосування пошукових методів і засобів у WEB-середовищі Тема 1. Web-простір, як середовище пошуку інформації 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. Рівень підготовки студентів оцінюється наступним чином: “Відмінно” (A) – відмінне виконання лише з незначною кількістю помилок; “Дуже добре” (B) – вище середнього рівня з кількома помилками; “Добре” (C) – у загальному правильна робота з певною кількістю грубих помилок; “Задовільно” (D) – непогано, але зі значною кількістю недоліків; “Достатньо” (E) – виконання задовольняє мінімальні критерії; “Незадовільно” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку; “Незадовільно” (F) – необхідна серйозна подальша робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра управління та інформаційно-аналітичного забезпечення оперативно-службової діяльності центру стратегічних комунікацій

Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій

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: - лекційних занять – 18 год. / 8 год. (заочна); - практичних (лабораторних) занять – 38 год. / 8 год (заочна); - самостійної роботи – 94 год. / 134 год. (заочна)
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (кіберзахист, забезпечення державної безпеки в інформаційній сфері), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог. ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН 16. Організувати 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.

		<p>ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення</p> <p>ПРН 22. Оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації</p> <p>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.</p> <p>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.</p>
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	<p>Змістовний модуль 1. Кіберзагрози. Основні аспекти виявлення та аналізу кіберзагроз</p> <ol style="list-style-type: none"> 1. Поняття та класифікація кіберзагроз. Моделі порушників та їх характеристики 2. Методи виявлення та аналізу кіберзагроз 3. Класифікація кіберзагроз. Налаштування мережевого моніторингу 4. Структура та основні функції систем виявлення вторгнень 5. SIEM-системи та їх роль у протидії кіберзагрозам 6. Методи кореляції та аналізу подій 7. Криптографічні методи протидії кіберзагрозам. Шифрування з симетричним та асиметричним ключем <p>Змістовний модуль 2. Засоби протидії кіберзагрозам</p> <ol style="list-style-type: none"> 1. Методи захисту критичної інформаційної інфраструктури. Приховування даних. Маскування даних. Стеганографія. 2. Методи протидії шкідливому програмному забезпеченню 3. Моделі захисту від атак соціальної інженерії. 4. DLP-системи та методи запобігання витоку даних 5. Моделі управління ризиками в кібербезпеці 6. Організація захисту кінцевих точок, основні методи. Модель «нульової довіри» Zero Trust. 7. Хмарна безпека, методи протидії загрозам у віртуалізованих середовищах 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	<p>Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, екзамен.</p> <p>Рівень підготовки студентів оцінюється наступним чином:</p> <p>“Відмінно” (A) – відмінне виконання лише з незначною кількістю помилок;</p> <p>“Дуже добре” (B) – вище середнього рівня з кількома помилками;</p> <p>“Добре” (C) – у загальному правильна робота з певною кількістю грубих помилок;</p> <p>“Задовільно” (D) – непогано, але зі значною кількістю недоліків;</p> <p>“Достатньо” (E) – виконання задовольняє мінімальні критерії;</p> <p>“Незадовільно” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;</p> <p>“Незадовільно” (F) – необхідна серйозна подальша робота.</p>
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

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: - лекційних занять – 38 год. / 10 год. (заочна); - практичних (лабораторних) занять – 38 год. / 14 год. (заочна); - самостійної роботи – 104 год. / 156 год. (заочна)
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності. ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН 12. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки і є основою для прийняття ефективних рішень, проведення досліджень та критичного осмислення проблем у галузі національної безпеки. ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання

		спеціалізованого програмного забезпечення ПРН 22. Оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації ПРН 26. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	Змістовний модуль 1. Технологічні підходи щодо інформаційної безпеки об'єктів критичної інфраструктури 1. Вимоги до кіберзахисту об'єктів критичної інфраструктури 2. Політика інформаційної безпеки на об'єктах критичної інфраструктури 3. Доступ користувачів до об'єктів критичної інфраструктури 4. Ідентифікація та автентифікація користувачів об'єкта критичної інфраструктури 5. Реєстрація подій та аудит об'єкта критичної інфраструктури Змістовний модуль 2. Мережевий захист компонентів та інформаційних ресурсів об'єктів критичної інформаційної інфраструктури 1. Мережевий захист об'єктів критичної інформаційної інфраструктури 2. Апаратні та програмні засоби мережевого захисту об'єктів критичної інформаційної інфраструктури 3. Аналіз захищеності мережевих об'єктів критичної інфраструктури 4. Використання бездротових мереж на об'єктах критичної інфраструктури Змістовний модуль 3. Технологічні та організаційні питання підтримки працездатності інформаційних ресурсів об'єктів критичної інфраструктури 1. Забезпечення відмовостійкості об'єктів критичної інфраструктури 2. Організаційні та технологічні питання підтримки працездатності інформаційних ресурсів об'єктів критичної інфраструктури 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,

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

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: - лекційних занять – 30 год. / 10 год. (заочна); - семінарських занять – 30 год. / 14 год. (заочна); - самостійної роботи – 120 год. / 156 год. (заочна)
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності. ПРН 3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (кіберзахист, забезпечення державної безпеки в інформаційній сфері), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог. ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових

		<p>стратегічних підходів.</p> <p>ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.</p> <p>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.</p>
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	<p>Змістовний модуль 1. Основи управління кіберінцидентами</p> <ol style="list-style-type: none"> 1. Поняття кіберінциденту та події інформаційної безпеки. Найвідоміші кіберінциденти в Україні та світі 2. Категоризація та життєвий цикл кіберінцидентів. 3. Джерела даних, методи та засоби виявлення кіберінцидентів 4. Виявлення подій. Знайомство з платформою MISP 5. Класифікація вразливостей комп'ютерних мереж та систем 6. Сортування та аналіз подій 7. Реагування та відновлення після кіберінциденту 8. Поліпшення можливостей в процесі управління подіями інформаційної безпеки. Ретроспектива <p>Змістовний модуль 2. Реагування на кіберінциденти</p> <ol style="list-style-type: none"> 1. Класифікація вразливостей інформаційних систем 2. Моніторинг подій інформаційної безпеки 3. Центри операційної безпеки, їх основні функції, структура та ролі. Команди реагування на кіберінциденти SERT/CSIRT, їх відмінності 4. Засоби реагування на кіберінциденти. Рішення для захисту кінцевих точок EDR/XDR, SIEM/SOAR/xSOAR 5. Аналіз інцидентів та цифрова криміналістика. Цифрові докази 6. Організаційні та правові аспекти розслідування кіберінцидентів 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	<p>Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, екзамен.</p> <p>Рівень підготовки студентів оцінюється наступним чином:</p> <p>“Відмінно” (A) – відмінне виконання лише з незначною кількістю помилок;</p> <p>“Дуже добре” (B) – вище середнього рівня з кількома помилками;</p> <p>“Добре” (C) – у загальному правильна робота з певною кількістю грубих помилок;</p> <p>“Задовільно” (D) – непогано, але зі значною кількістю недоліків;</p> <p>“Достатньо” (E) – виконання задовольняє мінімальні критерії;</p> <p>“Незадовільно” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку;</p> <p>“Незадовільно” (F) – необхідна серйозна подальша робота.</p>
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

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: - лекційних занять – 30 год. / 8 год (заочна); - семінарських занять – 30 год. / 8 год. (заочна); - самостійної роботи – 60 год. / 134 год. (заочна)
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності. ПРН 4. Організувати роботу колективу, забезпечувати професійний розвиток його членів та досягнення поставлених цілей. ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів. ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту,

		<p>технології створення та використання спеціалізованого програмного забезпечення</p> <p>ПРН 21. Досліджувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури</p> <p>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.</p>
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	<p>Змістовний модуль 1. Основи аудиту інформаційної безпеки та кібербезпеки</p> <ol style="list-style-type: none"> 1. Вступ до аудиту інформаційної безпеки та кібербезпеки: поняття, цілі, види 2. Крайні світові практики, стандарти і вимоги до проведення процедур аудиту інформаційної безпеки та кібербезпеки 3. Ризик-орієнтований підхід в аудиті інформаційної безпеки та кібербезпеки. 4. Аналіз політики інформаційної безпеки за стандартом ISO/IEC 27001, 27002, 27004 5. Правові аспекти аудиту інформаційної безпеки та кібербезпеки 6. Методологія та етапи проведення аудиту інформаційної безпеки та кібербезпеки 7. Методи та заходи планування процедур моніторингу операційних процесів установи 8. Аудит фізичної безпеки інформаційних систем, аудит управління доступом та аудит захисту від шкідливого програмного забезпечення. 9. Аудит безпеки систем промислової автоматизації (SCADA) <p>Змістовний модуль 2. Організація проведення аудиту інформаційної безпеки та кібербезпеки</p> <ol style="list-style-type: none"> 1. Організація процесу аудиту інформаційної безпеки та кібербезпеки. Ініціювання процедури аудиту 2. Послідовність дій та етапів аудиту інформаційної безпеки та кібербезпеки. Збір інформації для проведення аудиту та аналіз даних під час аудиту 3. Аналіз результатів аудиту та системи кібербезпеки. 4. Формування звітності на основі проведення аудиту інформаційної безпеки та кібербезпеки: документування результатів аудиту та підготовка аудиторського звіту 5. Концепція впровадження системи аудиту

		інформаційної безпеки в Україні (“Дорожня карта”) 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. Рівень підготовки студентів оцінюється наступним чином: “Відмінно” (A) – відмінне виконання лише з незначною кількістю помилок; “Дуже добре” (B) – вище середнього рівня з кількома помилками; “Добре” (C) – у загальному правильна робота з певною кількістю грубих помилок; “Задовільно” (D) – непогано, але зі значною кількістю недоліків; “Достатньо” (E) – виконання задовольняє мінімальні критерії; “Незадовільно” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку; “Незадовільно” (F) – необхідна серйозна подальша робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра кібербезпеки центру кібербезпеки

Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій

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: - лекційних занять – 20 год. / 6 год (заочна); - семінарських занять – 20 год. / 8 год. практичних (заочна); - самостійної роботи – 80 год. / 106 год (заочна)
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН 9. Синтезувати спектр заходів та підходів, що можуть використовуватись для вирішення проблем, пов'язаних з викликами глобальній, європейській та регіональній безпеці. ПРН 18. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. ПРН 21. Досліджувати системи та засоби

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

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

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

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: - лекційних занять – 30 год. / 8 год. (заочна); - семінарських занять – 30 год. / 6 год (заочна); - самостійної роботи – 60 год. / 106 год. (заочна)
7.	Програмні результати навчання	ПРН 3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (кіберзахист, забезпечення державної безпеки в інформаційній сфері), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог. ПРН 10. Формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності) (кіберзахист, забезпечення державної безпеки в інформаційній сфері). ПРН 13. Організувати та здійснювати керівництво територіальною обороною, мобілізаційною підготовкою та мобілізацією у межах професійної компетентності. ПРН 14. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються.

		<p>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.</p>
8.	Стислий зміст навчальної дисципліни (назва розділів, тем)	<p>Модуль 1. Теоретичні основи та елементи національного спротиву в Україні</p> <p>Тема 1. Особливості сучасного безпекового середовища України: роль і місце національного спротиву. Кіберрезерв сил територіальної оборони та руху опору України.</p> <p>Тема 2. Взаємодія і співпраця сил безпеки та оборони у системі національного спротиву. Структурно-функціональна модель організації територіальної оборони в Україні.</p> <p>Тема 3. Підготовка громадян України до національного спротиву. Кіберрезерв сил територіальної оборони.</p> <p>Модуль 2. Основи мобілізаційної підготовки та мобілізації в Україні.</p> <p>Тема 1. Основні принципи, зміст та організаційно-правові основи проведення мобілізаційної підготовки та мобілізації.</p> <p>Тема 2. Обов'язки підприємств, установ і організацій та громадян щодо мобілізаційної підготовки та мобілізації.</p> <p>Тема 3. Структура, зміст та порядок оформлення оперативного-мобілізаційних документів. Виконання мобілізаційних планів, завдань (замовлень) в умовах правового режиму воєнного стану.</p>
9.	Запланована навчальна діяльність та методи навчання	<p>Навчальна діяльність здійснюється шляхом лекційних, семінарських занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій.</p>
10.	Методи і критерії оцінювання	<p>Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, екзамен.</p> <p>Рівень підготовки студентів оцінюється наступним чином:</p> <p>“Відмінно” (А) – відмінне виконання лише з незначною кількістю помилок;</p> <p>“Дуже добре” (В) – вище середнього рівня з кількома помилками;</p> <p>“Добре” (С) – у загальному правильна робота з певною кількістю грубих помилок;</p> <p>“Задовільно” (D) – непогано, але зі значною</p>

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

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

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 протидія», «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: - самостійної роботи – 270 год.
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності. ПРН 3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (кіберзахист, забезпечення державної безпеки в

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

		<p>моделі захисту конфіденційності, організувати 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.</p> <p>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.</p> <p>ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення</p> <p>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.</p> <p>ПРН 21. Досліджувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури</p> <p>ПРН 22. Оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації</p> <p>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.</p> <p>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.</p> <p>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.</p>
8.	Стислий зміст навчальної дисципліни (назва	Змістовний модуль 1. Науково-дослідна практика Тема 1. Розробка індивідуального графіку

	розділів, тем)	<p>проходження практики. Узгодження його з науковим керівником кваліфікаційної (магістерської) роботи та керівником практики від кафедри.</p> <p>Тема 2. Визначення предмету та об'єкту дослідження, мети та завдань дослідження відповідно до закріпленої за здобувачем теми кваліфікаційної (магістерської) роботи</p> <p>Тема 3. Ознайомлення з науковими напрямами роботи на базі практики</p> <p>Тема 4. Ознайомлення з іноземними та вітчизняними науково-інформаційними джерелами за спеціалізацією, обрання наукової проблематики та формування бібліографії</p> <p>Тема 5. Збір та обробка даних щодо стану об'єкту дослідження на базі практики.</p> <p>Тема 6. Ознайомлення з нормативно-правовою документацією за обраною проблематикою та формування напрямів удосконалення стану об'єкту дослідження.</p> <p>Тема 7. Виконання індивідуального завдання відповідно до теми кваліфікаційної (магістерської) роботи</p> <p>Тема 8. Написання звіту з науково-дослідної практики</p>
	Запланована навчальна діяльність та методи навчання	<p>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.</p>
10.	Методи і критерії оцінювання	<p>Методами контролю є: індивідуальне і фронтальне опитування (усне та письмове), тестування, модульний контроль, диференційований залік.</p> <p>Рівень підготовки студентів оцінюється наступним чином:</p> <p>“Відмінно” (А) – відмінне виконання лише з незначною кількістю помилок;</p> <p>“Дуже добре” (В) – вище середнього рівня з кількома помилками;</p> <p>“Добре” (С) – у загальному правильна робота з певною кількістю грубих помилок;</p> <p>“Задовільно” (D) – непогано, але зі значною кількістю недоліків;</p> <p>“Достатньо” (Е) – виконання задовольняє мінімальні критерії;</p> <p>“Незадовільно” (FХ) – потрібно працювати перед тим, як отримати позитивну оцінку;</p>

		“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

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: - самостійної роботи – 180 год.
7.	Програмні результати навчання	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності. ПРН 3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (кіберзахист, забезпечення державної безпеки в

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

		<p>моделі захисту конфіденційності, організувати 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.</p> <p>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.</p> <p>ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення</p> <p>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.</p> <p>ПРН 21. Досліджувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури</p> <p>ПРН 22. Оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації</p> <p>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.</p> <p>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.</p> <p>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.</p>
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. Рівень підготовки студентів оцінюється наступним чином: “Відмінно” (A) – відмінне виконання лише з незначною кількістю помилок; “Дуже добре” (B) – вище середнього рівня з кількома помилками; “Добре” (C) – у загальному правильна робота з певною кількістю грубих помилок; “Задовільно” (D) – непогано, але зі значною кількістю недоліків; “Достатньо” (E) – виконання задовольняє мінімальні критерії; “Незадовільно” (FX) – потрібно працювати перед тим, як отримати позитивну оцінку; “Незадовільно” (F) – необхідна серйозна подальша робота.
11.	Мова навчання (українська та/або іноземні мови)	Українська
12.	Додаткова інформація (у разі потреби)	Немає

Кафедра кібербезпеки центру кібербезпеки

Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій