НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО”
ІНСТИТУТ СПЕЦІАЛЬНОГО ЗВ’ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ЗАТВЕРДЖЕНО
Методичною радою
КПІ ім. Ігоря Сікорського
(протокол № 8 від 20.06.2024 р.)

Ф-КАТАЛОГ

вибіркових навчальних дисциплін циклу професійної підготовки здобувачів ступеня **магістра** спеціальності 125 Кібербезпека та захист інформації за освітньо-професійною програмою

“Безпека державних інформаційних ресурсів”

РЕКОМЕНДОВАНО
Вченою радою ІСЗЗІ
КПІ ім. Ігоря Сікорського
(протокол № 12 від 16.05.2024 р.)

Київ
КПІ ім. Ігоря Сікорського
2024

ПЕРЕДМОВА

Цей каталог містить перелік та описи навчальних дисциплін, які рекомендуються до обрання здобувачами освіти, що навчаються на другому (магістерському) рівні вищої за освітньо-професійною програмою **“Безпека державних інформаційних ресурсів”** спеціальності 125 Кібербезпека та захист інформації.

Детальна інформація про правила й порядок обрання освітніх компонентів здобувачами освіти надана у Положенні про реалізацію права на вільний вибір навчальних дисциплін здобувачами вищої освіти ІСЗЗІ КПІ ім. Ігоря Сікорського другого (магістерського) рівня вищої освіти.

З урахуванням специфіки діяльності ІСЗЗІ КПІ ім. Ігоря Сікорського, як військового навчального підрозділу (військового Інституту) закладу вищої освіти, вибір здобувачами навчальних дисциплін реалізується шляхом анкетування.

Навчальні дисципліни, зазначені в цьому каталозі, можуть обирати також здобувачі освіти ІСЗЗІ КПІ ім. Ігоря Сікорського, які навчаються за іншими освітньо-професійними програмами та спеціальностями за умови виконання ними вимог до початку вивчення цих навчальних дисциплін.

Обрані здобувачем освіти навчальні дисципліни вносяться до його індивідуального навчального плану і стають обов’язковими для вивчення. Зміна вибіркових навчальних дисциплін після завершення встановлених термінів вибору не допускається.

Враховуючи особливості навчання за освітньо-професійними програмами підготовки на другому (магістерському) рівні вищої освіти, вибір навчальних дисциплін за цим каталогом здійснюється здобувачами після їх зарахування на навчання до ІСЗЗІ КПІ ім. Ігоря Сікорського наступним чином: відповідно до структури вибіркової складової навчального плану здобувачі освіти обирають дві вибіркові навчальні дисципліни обсягом по 4 кредити та три вибіркові навчальні дисципліни обсягом по 5 кредитів, які планують вивчати у другому семестрі першого року підготовки.

ЗМІСТ

Методи побудови та аналізу асиметричних криптосистем……....4
Правові засади захисту та стійкості критичної інфраструктури……...5
Менеджмент інформаційної безпеки держави……6
Менеджмент захисту інформаційного простору держави…….7
Основи наукових досліджень……...8
Криптографічні протоколи…….…..9
Системи кібербезпеки……..……10
Основи забезпечення безпеки та стійкості критичної інфраструктури…...11
Автоматизація проектування цифрових пристроїв……....12
Технології організації та захисту державних інформаційних ресурсів..…13
Прикладна криптографія…….…14

Методи побудови та аналізу асиметричних криптосистем	
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 1
Рівень вищої освіти	Другий (магістерський)
Курс, семестр	1 курс, весняний семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	4 кредити ЄКТС (120 годин), 60 годин аудиторної роботи, 60 годин самостійної роботи
Мова викладання	Українська
Вимоги до початку вивчення	Навчальна дисципліна відноситься до вибіркових компонентів циклу професійної підготовки освітньо-професійної програми підготовки магістрів. Для освоєння навчальної дисципліни здобувач повинен мати компетенції, отримані в результати освоєння таких навчальних дисциплін, як “Методи побудови та аналізу симетричних криптосистем”.
Що буде вивчатися?	Предметом навчальної дисципліни є основні державні та зарубіжні стандарти криптографічного захисту інформації, практичне використання отриманих знань для синтезу та аналізу асиметричних криптографічних систем.
Чому це цікаво/треба вивчати?	Наявність підрозділів у Держспецзв‘язку, які займаються проектуванням, розробкою, сертифікацією та ліцензуванням засобів криптографічного захисту інформації в автоматизованих системах. Застосування асиметричних алгоритмів шифрування у всіх сучасних інформаційно-комунікаційних системах.
Чому можна навчитися?	Програмні результати навчання, на формування та покращення яких спрямована дисципліна: інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах; провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі; застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки; аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення; досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури; ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик; планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки; проводити аналіз та синтез криптографічних алгоритмів та криптографічних протоколів; розробляти рекомендації впровадження інноваційних проектів, використовуючи базові методи дослідницької діяльності.
Як можна користуватися набутими знаннями і уміннями?	Метою навчальної дисципліни є формування та закріплення у курсантів наступних компетентностей: здатність застосовувати знання у практичних ситуаціях; здатність до абстрактного мислення, аналізу та синтезу; здатність до абстрактного мислення, аналізу та синтезуобґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки; здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки; здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації; здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на

	об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації; здатність аналізувати, інтегрувати і використовувати кращі світові практики, міжнародні стандарти при розробці криптографічних систем захисту інформації в спеціальних інформаційно-комунікаційних системах.
Інформаційне забезпечення	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали.
Вид семестрового контролю	Залік

Правові засади захисту та стійкості критичної інфраструктури

Кафедра, яка забезпечує викладання	Спеціальна кафедра № 1
Рівень вищої освіти	Другий (магістерський)
Курс, семестр	1 курс, весняний семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	4 кредити ЄКТС (120 годин), 60 годин аудиторної роботи, 60 годин самостійної роботи
Мова викладання	Українська
Вимоги до початку вивчення	Навчальна дисципліна відноситься до вибіркових компонентів циклу професійної підготовки освітньо-професійної програми підготовки магістрів. Для освоєння навчальної дисципліни здобувач повинен мати компетенції, отримані в результаті освоєння навчальної дисципліни “Ризик менеджмент критичної інфраструктури”.
Що буде вивчатися?	Предметом навчальної дисципліни є вивчення нормативно-правових актів в сфері забезпечення безпеки та стійкості критичної інфраструктури.
Чому це цікаво/треба вивчати?	- ознайомлення з законодавством України у сфері захисту об’єктів критичної інфраструктури; - вивчення основних засад та принципів державної політики у сфері захисту критичної інфраструктури; - аналіз нормативно-правової бази з питань правового регулювання безпеки на об’єктах критичної інфраструктури; - дослідження основних принципів реалізації державних цільових програм із захисту критичної інфраструктури; - отримання навиків з комплексу заходів з виявлення, запобігання та ліквідації наслідків інцидентів на об’єктах критичної інфраструктури України; - встановлення обов’язкових вимог із забезпечення безпеки об’єктів критичної інфраструктури, їхньої захищеності на всіх етапах життєвого циклу, в тому числі під час створення, введення до експлуатації, модернізації.
Чому можна навчитися?	Програмні результати навчання, на формування та покращення яких спрямована дисципліна: досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури; забезпечувати безпеку та стійкість об’єктів критичної інфраструктури, запобігати проявам несанкціонованого втручання в їх функціонування, прогнозування та запобігання кризовим ситуаціям на об’єктах критичної інфраструктури.
Як можна користуватися набутими знаннями і уміннями?	Метою навчальної дисципліни є формування та закріплення у курсантів наступних компетентностей: здатність аналізувати, контролювати та забезпечувати формування та реалізацію державної політики у сфері захисту критичної інфраструктури.
Інформаційне забезпечення	Робоча програма навчальної дисципліни (Силабус), навчально-методичні розробки
Вид семестрового контролю	Залік

Менеджмент інформаційної безпеки держави	
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 1
Рівень вищої освіти	Другий (магістерський)
Курс, семестр	1 курс, весняний семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ЄКТС (150 годин), 72 години аудиторної роботи, 78 годин самостійної роботи
Мова викладання	Українська
Вимоги до початку вивчення	Успішне вирішення завдань навчальної дисципліни базується на засвоєні здобувачами знань та умінь, сформованих у них, в результаті вивчення навчальних дисциплін бакалаврського рівня вищої освіти, а також “Інтелектуальна власність та патентознавство” та підсилює вивчення навчальної дисципліни “Ризик-менеджмент критичної інфраструктури”, цей курс забезпечує професійне спрямування процесу навчання здобувачів та отримання ними нових знань та навичок.
Що буде вивчатися?	Предметом навчальної дисципліни є система забезпечення інформаційної безпеки держави що функціонує, а також застосування форм і методів організації захисту особового складу від негативного інформаційно-психологічного впливу.
Чому це цікаво/треба вивчати?	Дає можливість комплексного застосування знань з питань Менеджменту інформаційної безпеки держави у вирішенні службових, професійних завдань та прийнятті управлінських рішень.
Чому можна навчитися?	Програмні результати навчання, на формування та покращення яких спрямована дисципліна: РН2 Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН4 Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН9 Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
Як можна користуватися набутими знаннями і уміннями?	Метою навчальної дисципліни є формування у курсантів наступних компетентностей: КЗ-1 Здатність застосовувати знання у практичних ситуаціях. КЗ-3 Здатність до абстрактного мислення, аналізу та синтезу. КФ4 Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
Інформаційне забезпечення	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали.
Вид семестрового контролю	Залік

Менеджмент захисту інформаційного простору держави	
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 4
Рівень вищої освіти	Другий (магістерський)
Курс, семестр	1 курс, весняний семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ЄКТС (150 годин), 72 години аудиторної роботи, 78 годин самостійної роботи
Мова викладання	Українська
Вимоги до початку вивчення	Успішне вирішення завдань навчальної дисципліни базується на засвоєні здобувачами знань та умінь, сформованих у них, в результаті вивчення навчальних дисциплін бакалаврського рівня вищої освіти а також “Інтелектуальна власність та патентознавство” та підсилює вивчення навчальної дисципліни “Ризик-менеджмент критичної інфраструктури”, цей курс забезпечує професійне спрямування процесу навчання здобувачів та отримання ними нових знань та навичок
Що буде вивчатися?	Предметом навчальної дисципліни є питання захисту інформаційного простору України.
Чому це цікаво/треба вивчати?	Дає можливість комплексного застосування знань з питань менеджменту захисту інформаційного простору держави у вирішенні службових, професійних завдань та прийнятті управлінських рішень.
Чому можна навчитися?	Програмні результати навчання, на формування та покращення яких спрямована дисципліна: РН2 Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН17 Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об’єктивно оцінювати результати навчання.
Як можна користуватися набутими знаннями і уміннями?	Метою навчальної дисципліни є формування у курсантів наступних компетентностей: КЗ-1 Здатність застосовувати знання у практичних ситуаціях. КЗ-3 Здатність до абстрактного мислення, аналізу та синтезу. КФ2 Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
Інформаційне забезпечення	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали.
Вид семестрового контролю	Залік

Основи наукових досліджень	
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 4
Рівень вищої освіти	Другий (магістерський)
Курс, семестр	1 курс, весняний семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ЄКТС (150 годин), 72 години аудиторної роботи, 78 годин самостійної роботи
Мова викладання	Українська
Вимоги до початку вивчення	Навчальна дисципліна відноситься до вибіркових компонентів циклу професійної підготовки освітньо-професійної програми підготовки магістрів. Успішне вирішення завдань навчальної дисципліни базується на засвоєні здобувачами знань та умінь, сформованих у них, в результаті вивчення навчальних дисциплін бакалаврського рівня вищої освіти, а також “Інтелектуальна власність та патентознавство” та підсилює вивчення навчальної дисципліни “Ризик-менеджмент критичної інфраструктури”, цей курс забезпечує професійне спрямування процесу навчання здобувачів та отримання ними нових знань та навичок
Що буде вивчатися?	Предметом навчальної дисципліни “Основи наукових досліджень” є загальні закономірності розвитку науки; сутність наукового пізнання, філософські засади, принципи, методи, види, форми, рівні та норми наукового пізнання; особливості воєнно-наукового і професійного пізнання.
Чому це цікаво/треба вивчати?	Дає можливість комплексного застосування знань з питань захисту інформаційного простору України у вирішенні службових, професійних завдань та прийнятті управлінських рішень.
Чому можна навчитися?	Програмні результати навчання, на формування та покращення яких спрямована дисципліна: РН3 Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. РН15 Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб..
Як можна користуватися набутими знаннями і уміннями?	Метою навчальної дисципліни є формування у курсантів наступних компетентностей: КЗ-3 Здатність до абстрактного мислення, аналізу та синтезу. КЗ-4 Здатність оцінювати та забезпечувати якість виконуваних робіт. КФ10 Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
Інформаційне забезпечення	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали.
Вид семестрового контролю	Залік

Криптографічні протоколи

Кафедра, яка забезпечує викладання	Спеціальна кафедра № 1
Рівень вищої освіти	Другий (магістерський)
Курс, семестр	1 курс, весняний семестр
Обсяг дисципліни та розподіл годин	4 кредити ЄКТС (120 годин), 60 годин аудиторної роботи, 60 годин самостійної роботи
Мова викладання	Українська
Вимоги до початку вивчення	Навчальна дисципліна відноситься до вибіркових компонентів циклу професійної підготовки освітньо-професійної програми підготовки магістрів. Для освоєння навчальної дисципліни здобувач повинен мати компетенції, отримані в результати освоєння таких навчальних дисциплін, як: “Методи побудови та аналізу симетричних криптосистем”.
Що буде вивчатися?	Предмет навчальної дисципліни є застосування криптографічних протоколів для забезпечення послуг інформаційної безпеки. Зміст навчальної дисципліни: сучасні стандарти у галузі криптографічного захисту інформації; основні схеми цифрового підпису та хешування; протоколи аутентифікації; протоколи передачі та розподілення ключів; криптографічні протоколи різних рівнів моделі OSI та основні вимоги до них.
Чому це цікаво/треба вивчати?	Криптографічні протоколи використовуються для захисту конфіденційності, цілісності та автентичності інформації. Дослідження цих протоколів дозволяє створювати та аналізувати безпечні системи, які запобігають несанкціонованому доступу до даних та захищають їх від несанкціонованих змін.
Чому можна навчитися?	Навчальна дисципліна спрямована на підсилення наступних результатів навчання: інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах; провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі; аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення; досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури; ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик; планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки; використовувати результати аналізу кращих світових практик, стандартів із захисту інформації при розробці криптографічних систем захисту інформації в спеціальних інформаційно-комунікаційних системах.
Як можна користуватися набутими знаннями і уміннями?	Метою навчальної дисципліни є формування та закріплення у курсантів наступних компетентностей: здатність застосовувати знання у практичних ситуаціях; Здатність проводити дослідження на відповідному рівні; здатність до абстрактного мислення, аналізу та синтезу; здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності); здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки; здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки; здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури; здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації; здатність досліджувати, розробляти, впроваджувати та

	супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації; здатність аналізувати, інтегрувати і використовувати кращі світові практики, міжнародні стандарти при розробці криптографічних систем захисту спеціальних інформаційно-комунікаційних систем.
Інформаційне забезпечення	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали.
Вид семестрового контролю	Залік

Системи кібербезпеки

Кафедра, яка забезпечує викладання	Спеціальна кафедра № 1
Рівень вищої освіти	Другий (магістерський)
Курс, семестр	1 курс, весняний семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ЄКТС (150 годин), 72 години аудиторної роботи, 78 годин самостійної роботи
Мова викладання	Українська
Вимоги до початку вивчення	Навчальна дисципліна відноситься до вибіркових компонентів циклу професійної підготовки освітньо-професійної програми підготовки магістрів. Для освоєння навчальної дисципліни здобувач повинен мати компетенції, отримані в результати освоєння таких навчальних дисциплін, як: "Технології виявлення та блокування загроз державним інформаційним ресурсам в інформаційно-комунікаційних системах".
Що буде вивчатися?	Предметом навчальної дисципліни є вивчення систем управління інцидентами та подіями інформаційної безпеки та систем захисту державних інформаційних ресурсів.
Чому це цікаво/треба вивчати?	Зростає кількість кіберзагроз та складність шкідливого програмного забезпечення, що вимагає розвитку та впровадження стандартів і протоколів для регулювання систем управління інформаційною безпекою. Захист державних інформаційних ресурсів та особистих даних користувачів стає критично важливим у цьому контексті.
Чому можна навчитися?	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. 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.
Як можна користуватися набутими знаннями і уміннями?	Здатність реалізовувати технічні вимоги на основі технік оцінки рівня захищеності інформаційних систем, технологій аналізу мережевого трафіку та принципів протидії кібератакам. Здатність аналізувати, контролювати та забезпечувати формування та реалізацію державної політики у сфері захисту критичної інфраструктури.
Інформаційне забезпечення	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали.
Вид семестрового контролю	Залік

Основи забезпечення безпеки та стійкості критичної інфраструктури

Кафедра, яка забезпечує викладання	Спеціальна кафедра № 1
Рівень вищої освіти	Другий (магістерський)
Курс, семестр	1 курс, весняний семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ЄКТС (150 годин), 72 години аудиторної роботи, 78 годин самостійної роботи
Мова викладання	Українська
Вимоги до початку вивчення	Навчальна дисципліна відноситься до вибіркових компонентів циклу професійної підготовки освітньо-професійної програми підготовки магістрів. Для освоєння навчальної дисципліни здобувач повинен мати компетенції, отримані в результати освоєння таких навчальних дисциплін, як: “Ризик менеджмент критичної інфраструктури”.
Що буде вивчатися?	Предметом навчальної дисципліни є вивчення принципів, методів та засобів захисту критичних інфраструктур від різноманітних загроз і ризиків.
Чому це цікаво/треба вивчати?	Забезпечення національної безпеки: критична інфраструктура є основою функціонування сучасного суспільства. Її захист від загроз є ключовим елементом національної безпеки; відмови або руйнування критичних систем можуть призвести до серйозних економічних і соціальних наслідків, включаючи втрату життя. Запобігання катастрофам: знання про загрози та ризики допомагає розробляти ефективні стратегії запобігання та реагування на надзвичайні ситуації; це включає підготовку до природних катастроф, техногенних аварій, кібератак тощо. Підтримка економічної стабільності: надійна та стійка критична інфраструктура є основою для стабільного функціонування економіки; захист інфраструктури від збоїв допомагає запобігти економічним втратам та підтримувати нормальну діяльність бізнесу і державних установ.
Чому можна навчитися?	Навчальна дисципліна спрямована на підсилення наступних результатів навчання: забезпечувати безпеку та стійкістб об’єктів критичної інфраструктури, запобігати проявам несанкціонованого втручання в їх функціонування, прогнозування та запобігання кризовим ситуаціям на об’єктах критичної інфраструктури. Вивчення цієї дисципліни допомагає здобувачам стати фахівцями, здатними забезпечувати надійність і безпеку важливих систем і об'єктів, що є критичними для функціонування сучасного суспільства.
Як можна користуватися набутими знаннями і уміннями?	Метою навчальної дисципліни є формування та закріплення у курсантів наступних компетентностей: Здатність аналізувати, контролювати та забезпечувати формування та реалізацію державної політики у сфері захисту критичної інфраструктури.
Інформаційне забезпечення	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали.
Вид семестрового контролю	Залік

Автоматизація проектування цифрових пристроїв

Кафедра, яка забезпечує викладання	Спеціальна кафедра № 1
Рівень вищої освіти	Другий (магістерський)
Курс, семестр	1 курс, весняний семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ЄКТС (150 годин), 72 години аудиторної роботи, 78 годин самостійної роботи
Мова викладання	Українська
Вимоги до початку вивчення	Навчальна дисципліна відноситься до вибіркових компонентів циклу професійної підготовки освітньо-професійної програми підготовки магістрів. Для освоєння навчальної дисципліни здобувач повинен мати компетенції, отримані в результаті освоєння таких навчальних дисциплін, як: “Методи побудови та аналізу симетричних криптосистем”; “Методологічні засади захисту інформації від витоку технічними каналам”.
Що буде вивчатися?	Предметом навчальної дисципліни є вивчення основ застосування сучасних методів автоматизованого синтезу та аналізу цифрових комбінаційних та послідовних схем, інструментів, програмних середовищ, систем автоматизованого проектування (САПР) типу MAX+plus II, Quartus II, ModelSim та HDL мов опису (Verilog та VHDL), методів автоматизованого проектування та моделювання складних цифрових пристроїв, таких як програмуємі логічні інтегральні мікросхеми (ПЛІС).При вивченні практичних підходів до автоматизованого проектування цифрових засобів, поглиблена увага приділяється прикладам проектуванню цифрових пристроїв для засобів захисту інформації.
Чому це цікаво/треба вивчати?	Наявність у Держспецзв'язку підрозділів, що вирішують завдання з розробки та проектування цифрових засобів захисту інформації. Для вирішення таких завдань дисципліна забезпечує формування теоретико-практичних основ та знання стандартів в галузі автоматизованого проектування цифрових пристроїв (ЦП) засобів захисту інформації та спрямована на глибоке вивчення теорії та практики автоматизованого проектування ЦП на основі застосування систем автоматизованого проектування типу типу MAX+plus II, Quartus II, ModelSim та HDL мов поведінкового опису ЦП Verilog і VHDL для їх розробки та моделювання.
Чому можна навчитися?	Програмні результати навчання, на формування та покращення яких спрямована дисципліна: провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі; застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки; досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури; ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
Як можна користуватися набутими знаннями і уміннями?	Метою навчальної дисципліни є формування та закріплення у курсантів наступних компетентностей: здатність застосовувати знання у практичних ситуаціях; здатність до абстрактного мислення, аналізу та синтезу; здатність до абстрактного мислення, аналізу та синтезу обґрунтовано застосовувати, інтегрувати, розробляти та вдосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки; здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури; здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Інформаційне забезпечення	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали, електронні посібники.
Вид семестрового контролю	Залік

Технології організації та захисту державних інформаційних ресурсів

Кафедра, яка забезпечує викладання	Спеціальна кафедра № 1
Рівень вищої освіти	Другий (магістерський)
Курс, семестр	1 курс, весняний семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ЄКТС (150 годин), 72 години аудиторної роботи, 78 годин самостійної роботи
Мова викладання	Українська
Вимоги до початку вивчення	Навчальна дисципліна відноситься до вибіркових компонентів циклу професійної підготовки освітньо-професійної програми підготовки магістрів. Для освоєння навчальної дисципліни здобувач повинен мати компетенції, отримані в результати освоєння таких навчальних дисциплін, як: “Технології виявлення та блокування загроз державним інформаційним ресурсам в інформаційно-комунікаційних системах”.
Що буде вивчатися?	Предметом навчальної дисципліни є вивчення системи аналізу шкідливого програмного забезпечення та системи аналізу інцидентів.
Чому це цікаво/треба вивчати?	Кількість і складність кіберзагроз постійно збільшується, що підвищує необхідність розуміння технологій захисту для ефективної протидії цим загрозам і мінімізації ризиків. Вивчення технологій безпеки дозволяє забезпечити конфіденційність і цілісність даних. Державні інформаційні ресурси часто містять критичну для національної безпеки інформацію, тому їх захист є ключовим для стабільності та безпеки країни.
Чому можна навчитися?	Використовувати методи натурного, фізичного і комп’ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. Оцінювати стан інформаційних систем, розподіляти послуги безпеки і обирати механізми безпеки, впроваджувати технологічні рішення інноваційного характеру щодо виявлення та блокування загроз інформаційним ресурсам.
Як можна користуватися набутими знаннями і уміннями?	Здатність 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. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
Інформаційне забезпечення	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали
Вид семестрового контролю	Залік

Прикладна криптографія

Кафедра, яка забезпечує викладання	Спеціальна кафедра № 1
Рівень вищої освіти	Другий (магістерський)
Курс, семестр	1 курс, весняний семестр
Обсяг дисципліни та розподіл годин	4 кредити ЄКТС (120 годин), 60 годин аудиторної роботи, 60 годин самостійної роботи
Мова викладання	Українська
Вимоги до початку вивчення	Навчальна дисципліна відноситься до вибіркових компонентів циклу професійної підготовки освітньо-професійної програми підготовки магістрів. Для освоєння навчальної дисципліни здобувач повинен мати компетенції, отримані в результати освоєння таких навчальних дисциплін, як: “Методи побудови та аналізу симетричних криптосистем”.
Що буде вивчатися?	Предмет навчальної дисципліни є застосування криптографічних протоколів різних рівнів моделі OSI для побудови захищених інформаційно-комунікаційних систем. Зміст навчальної дисципліни: модель протоколів TCP/IP; архітектура E-MAIL; сценарії протоколу PGP; структура протоколу MIME; алгоритми зміни ключів, шифрування, розшифрування, ґешування та стиску протоколу SSL; протокол TLS; транспортний та тунельний режими роботи IPSec; протоколи AH та ESP; удосконалений протокол управління ключами Діффі-Хелмана. фази протоколу IKE; протокол ISAKMP.
Чому це цікаво/треба вивчати?	Криптографічні протоколи різних рівнів моделі OSI використовуються для забезпечення конфіденційності, цілісності та автентичності інформації. Дослідження цих протоколів дозволяє створювати та аналізувати інформаційно-комунікаційні системи, які запобігають несанкціонованому доступу до даних та захищають їх від несанкціонованих змін.
Чому можна навчитися?	Навчальна дисципліна спрямована на підсилення наступних результатів навчання: інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах; провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі; аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення; досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури; ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик; планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки; використовувати результати аналізу кращих світових практик, стандартів із захисту інформації при розробці криптографічних систем захисту інформації в спеціальних інформаційно-комунікаційних системах.
Як можна користуватися набутими знаннями і уміннями?	Метою навчальної дисципліни є формування та закріплення у курсантів наступних компетентностей: здатність застосовувати знання у практичних ситуаціях; Здатність проводити дослідження на відповідному рівні; здатність до абстрактного мислення, аналізу та синтезу; здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності); здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки; здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки; здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури; здатність аналізувати, контролювати та забезпечувати систему управління доступом до

	інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації; здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації; здатність аналізувати, інтегрувати і використовувати кращі світові практики, міжнародні стандарти при розробці криптографічних систем захисту спеціальних інформаційно-комунікаційних систем.
Інформаційне забезпечення	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали.
Вид семестрового контролю	Залік