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 122 Комп’ютерні науки

за освітньо-професійною програмою
“Комп’ютерні системи і технології спеціального зв’язку”

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 **“Комп’ютерні системи і технології спеціального зв’язку”** спеціальності 122 Комп’ютерні науки.

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

Технології організації захисту державних інформаційних ресурсів 4
Радіоелектронний захист систем електронних комунікацій 5
Технології та методи захисту інформаційно-комунікаційних систем від кібератак 6
Системи кібербезпеки 7
Моніторинг та управління спеціальними інформаційно-комунікаційними системами 8
Основи IT-аудиту.....9
Менеджмент інформаційної безпеки держави 10
Інтернет речей та безпека Інтернет-ресурсів.....11
Фреймворки управління ризиками інформаційної безпеки.....12
Математичні методи побудови та аналізу асиметричних криптосистем.....13
Планування та проектування транспортних спеціальних систем електронних комунікацій.....14
Моделювання систем управління інформаційною безпекою.....15
Автоматизація проектування цифрових пристроїв.....16
Сучасні інформаційні технології передачі даних в інформаційних системах 17
Математичне моделювання процесів та систем.....18

Технології організації захисту державних інформаційних ресурсів	
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 1
Рівень вищої освіти	Другий (магістерський)
Курс, семестр	1 курс, весняний (2) 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	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 дисципліни	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали
Вид семестрового контролю	Залік

Радіоелектронний захист систем електронних комунікацій	
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 3
Рівень вищої освіти	Другий (магістерський)
Курс, семестр	1 курс, весняний (2) 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 курсантами знань та умінь, сформованих у них, в результаті вивчення таких навчальних дисциплін: “Уніфіковані мережі інформаційно-комунікаційних систем”, цей курс забезпечує професійне спрямування процесу навчання здобувачів та отримання ними нових навичок.
Що буде вивчатися?	Предметом навчальної дисципліни є принципи, методи та способи забезпечення стійкої роботи спеціальних електронних комунікацій в мирний час, в умовах надзвичайного стану та в особливий період. Метою навчальної дисципліни є оволодіння принципами, методами та способами захисту електронних комунікацій від: радіоелектронної розвідки, навмисних радіоелектронних завад, ураження високоточною зброєю, взаємних завад, іонізуючого та електромагнітного випромінювання, деструктивного комп’ютерного впливу, що здійснюється по радіоканалу.
Чому це цікаво / треба вивчати?	Дає можливість розв’язувати нагальні та оригінальні задачі у сфері спеціальних систем електронних комунікацій, особливо при їх застосуванні в умовах надзвичайного стану та в особливий період.
Чому можна навчитися?	✓ проводити аналіз сигнально-завадової обстановки та здійснювати оцінку можливостей противника по веденню радіоелектронної розвідки; ✓ визначати зони радіорозвідки та радіоподавлення комплексів (засобів) радіоелектронної боротьби в інформаційних конфліктах в електромагнітному спектрі; ✓ розраховувати основні показники завадостійкості спеціальних засобів зв’язку; ✓ розробляти пропозиції щодо радіоелектронного захисту засобів зв’язку в умовах застосування навмисних завад. ✓ визначати перспективні напрямки радіоподавлення та радіоелектронного захисту спеціальних засобів зв’язку; ✓ налаштовувати інструменти захисту сучасних радіозасобів спеціального призначення; ✓ створювати математичні та імітаційні моделі для оцінки завадостійкості засобів; ✓ проводити тестування телекомунікаційних радіомереж на стійкість до деструктивного комп’ютерного впливу, що здійснюється по радіоканалу; ✓ визначати заходи з радіоелектронного захисту.
Як можна користуватися набутими знаннями і уміннями?	Застосовувати під час виконання завдань за призначенням із застосування спеціальних електронних комунікацій в умовах надзвичайного стану та в особливий період період, при проведенні наукових досліджень у сфері радіоелектронного та кібернетичного захисту спеціальних систем електронних комунікацій.
Інформаційне забезпечення дисципліни	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали
Вид семестрового контролю	Залік

Технології та методи захисту інформаційно-комунікаційних систем від кібератак	
Кафедра	Спеціальна кафедра № 5
Рівень вищої освіти	Другий (магістерський)
Курс, семестр	1 курс, весняний (2) 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	Для освоєння дисципліни здобувач повинен мати компетенції, отримані в результаті освоєння таких дисциплін як: “Сучасні технології програмування”, “Адміністрування та захист систем управління базами даних”
Що буде вивчатися?	Перша частина присвячена вивченню вимог міжнародних стандартів, технологій кіберзахисту та моніторингу ІКС. Друга частина націлена на вивчення технологій міжмережевих екранів та систем виявлення та попередження вторгнень. Третя частина - структура, функції та програмне забезпечення сучасного центру кіберзахисту.
Чому це цікаво / треба вивчати?	Кібербезпека є критично важливою сферою, яка охоплює захист інформаційних систем від зловмисних атак і загроз. Вивчення вимог міжнародних стандартів, технологій кіберзахисту та моніторингу інформаційних систем дозволяє ефективно захищати свої дані та мережі. Технології міжмережевих екранів і систем виявлення та попередження вторгнень забезпечують контроль доступу і фільтрацію трафіку, допомагаючи виявляти та запобігати атакам. Сучасні центри кіберзахисту (SOC) забезпечують централізоване управління безпекою, постійний моніторинг і швидке реагування на інциденти, використовуючи сучасне програмне забезпечення для збору та аналізу даних. Вивчення цих тем є необхідним для підготовки фахівців, здатних забезпечити надійний захист інформаційних систем в умовах зростаючих кіберзагроз.
Чому можна навчитися?	Результати навчання : 1. Мати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері комп’ютерних наук і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем у сфері комп’ютерних наук та на межі галузей знань. 2. Мати спеціалізовані уміння/навички розв’язання проблем комп’ютерних наук, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур. 3. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію у сфері комп’ютерних наук до фахівців і нефахівців, зокрема до осіб, які навчаються. 4. Проєктувати архітектурні рішення інформаційних та комп’ютерних систем різного призначення. 5. Аналізувати сучасний стан і світові тенденції розвитку комп’ютерних наук та інформаційних технологій.
Як можна користуватися набутими знаннями і уміннями?	1. Розробляти, описувати, аналізувати та оптимізувати архітектурні рішення інформаційних та комп’ютерних систем різного призначення 2. Забезпечувати захист інформації в інформаційних, електронних комунікаційних, інформаційно-комунікаційних системах та кіберзахист об’єктів критичної інфраструктури, використовувати сучасні методології моделювання систем управління інформаційною безпекою, фреймворки управління ризиками інформаційної безпеки та кібербезпеки.
Інформаційне забезпечення дисципліни	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 (2) 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	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 дисципліни	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали
Вид семестрового контролю	Залік

Моніторинг та управління спеціальними інформаційно-комунікаційними системами	
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 3
Рівень вищої освіти	Другий (магістерський)
Курс, семестр	1 курс, весняний (2) 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 курсантами знань та умінь, сформованих у них, в результаті вивчення навчальних дисциплін пов'язаних з вивченням інформаційно-комунікаційних систем.
Що буде вивчатися?	Предметом навчальної дисципліни є принципи, методи забезпечення електромагнітної сумісності за завадозахисту РЕЗ, організаційні та правові засади використання радіочастотного ресурсу в Держспецзв'язку.
Чому це цікаво / треба вивчати?	Метою навчальної дисципліни є оволодіння основними поняттями, правовими нормами, принципами користування радіочастотним ресурсом із врахуванням рішення основних проблем електромагнітної сумісності.
Чому можна навчитися?	✓ проводити аналіз електромагнітної обстановки та здійснювати оцінку основних технічних факторів, що впливають на ЕМС; ✓ проводити розрахунок об'єктової ЕМС та організовувати натурні випробування щодо ЕМС РЕЗ; ✓ організувати експлуатацію та обслуговування основних засобів радіочастотного контролю; ✓ розраховувати основні показники завадостійкості; ✓ проводити аналіз сигнально-завадової обстановки та здійснювати оцінку можливостей противника по веденню радіоелектронної розвідки; ✓ визначати зони радіорозвідки та радіоподавлення комплексів (засобів) радіоелектронної боротьби в інформаційних конфліктах в електромагнітному спектрі; ✓ розробляти пропозиції щодо розраховувати основні показники завадостійкості спеціальних засобів зв'язку.
Як можна користуватися набутими знаннями і уміннями?	✓ Організовувати пошук та усунення джерел завад РЕЗ Держспецзв'язку; ✓ Використовувати радіочастотні ресурси в умовах надзвичайного або воєнного стану; ✓ Визначати перспективні напрямки радіоподавлення та радіоелектронного захисту спеціальних засобів зв'язку, а також, налаштовувати інструменти захисту сучасних радіо засобів тастворювати математичні та імітаційні моделі для оцінки завадостійкості засобів зв'язку.
Інформаційне забезпечення дисципліни	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали
Вид семестрового контролю	Залік

Основи IT-аудиту	
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 5
Рівень вищої освіти	Другий (магістерський)
Курс, семестр	1 курс, весняний (2) 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	. Для освоєння дисципліни здобувач повинен мати компетенції, отримані в результаті освоєння таких дисциплін та практик як: “Інформаційні технології в національній системі кібербезпеки”, “Адміністрування та захист систем управління базами даних”, “Забезпечення якості та реверс-інжиніринг програмного забезпечення” “Сучасні технології програмування”, “Розподілені обчислювальні системи”, “ Кібернавчання”.
Що буде вивчатися?	Система комплексних знань та інформаційних технологій, які застосовуються для керування кібербезпекою та аудиту захищених комп’ютерних систем. Заходи та засоби організації сучасної інфраструктури кіберзахисту для інформаційних систем, що оброблюють державні інформаційні ресурси або інформацію з обмеженим доступом.
Чому це цікаво / треба вивчати?	Розроблення, впровадження та експлуатація сучасних інформаційних технологій в самих різних сферах діяльності суспільства обов’язково супроводжується необхідністю виконанням вимог щодо забезпечення ефективного рівня кібербезпеки. Становлення конкурентоспроможного IT фахівця неможливо без комплексного розуміння сутності процесів кіберзахисту, принципів їх реалізації.
Чому можна навчитися?	Тематика занять дисципліни дозволяє сформувати компетенції щодо: формування аналізу ризиків кіберзагроз інформаційної технології на основі проведення тестування на проникнення; визначення структури та конкретного складу інфраструктури кіберзахисту різних видів інформаційних систем (адміністративних IT-system, промислових ICS типу PLC, DCS, SCADA). Також фахівці отримають навички організації та проведення об’єктивного аудиту безпеки інформаційних технологій.
Як можна користуватися набутими знаннями і уміннями?	Здобувачі вищої освіти після засвоєння навчальної дисципліни мають продемонструвати такі програмні результати навчання: - спеціалізовані знання концепцій, політик та методологій застосування комп’ютерних технологій забезпечення обробки держаних інформаційних ресурсів; - спеціалізовані уміння/навички розв’язання проблем застосування захищених комп’ютерних технологій критичної інформаційної інфраструктури; - уміння управляти робочими процесами (розвідка кіберзагроз, кіберзахист, аудит безпеки) у сфері інформаційних технологій для обробки державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, які є складними та потребують нових стратегічних підходів.
Інформаційне забезпечення дисципліни	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали
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 (2) 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	Для освоєння навчальної дисципліни здобувач повинен мати компетенції, отримані в результати освоєння таких навчальних дисциплін, як: “Інтелектуальна власність та патентознавство”, “Технології виявлення та блокування загроз державним інформаційним ресурсам в інформаційно-комунікаційних системах”, “Методи побудови та аналізу симетричних криптосистем”, “Математичні методи оптимізації та моделювання”, “Ризик-менеджмент критичної інфраструктури”.
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 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: Провадити дослідницьку та інноваційну діяльність в сфері інформаційної безпеки або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі; Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та кібербезпекою організації на базі стратегії і політики інформаційної безпеки; Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, операційних процесів у сфері інформаційної та кібербезпеки в цілому; Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та кібербезпеки, а також знання та пояснення, що їх обгрунтовують до персоналу, партнерів та інших осіб; Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.
Як можна користуватися набутими знаннями і уміннями?	Метою навчальної дисципліни є формування у курсантів наступних компетентностей: Здатність застосувати знання у практичних ситуаціях; Здатність проводити дослідження на відповідному рівні, застосувати знання у практичних ситуаціях; Здатність до абстрактного мислення, аналізу і синтезу; Здатність до ефективних комунікаційних взаємодій, в тому числі засобами інформаційних технологій.
Інформаційне забезпечення дисципліни	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали
Вид семестрового контролю	Залік

Інтернет речей та безпека Інтернет-ресурсів	
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 5
Рівень вищої освіти	Другий (магістерський)
Курс, семестр	1 курс, весняний (2) 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	Для освоєння дисципліни здобувач повинен мати компетенції, отримані в результаті освоєння таких дисциплін як: “WEB-орієнтована розробка програмного забезпечення”, “Адміністрування та захист систем управління базами даних”, “Сучасні технології програмування”, “Безпека інформаційних систем ”
Що буде вивчатися?	Сучасні методи та підходи забезпечення безпеки інформації в автоматизованих інформаційних системах, основу яких складають ресурси з віддаленим доступом, принципи розробки захищених вебзастосунків, технологій забезпечення безпеки Інтернет-ресурсів, засоби аналіз захищеності інформаційних ресурсів. Архітектура Інтернету речей. Протоколи та інтерфейси обміну даними між пристроями Інтернету речей.
Чому це цікаво / треба вивчати?	Швидкий розвиток інформаційних систем з доступом через мережу Інтернет, а також розумних речей і їх робота в Інтернет потребує глибоких знань принципів та технологій реалізації відповідних ресурсів. Для забезпечення безпеки функціонування важливо розуміти загрози та ризики та приймати відповідні заходи для їх запобігання.
Чому можна навчитися?	Результати навчання: знання правил, алгоритмів та методів налагодження безпеки Інтернет-ресурсів; сервіс-орієнтованих середовищ та екосистеми Інтернету речей; підходів до тестування та відладки апаратно-програмних комплексів інформаційних систем; вміння забезпечувати захист і оцінку захищеності спеціальних інформаційних систем; досвід проведення тестування вебзастосувань з метою пошуку вразливостей; використання технологій запобігання атакам на Інтернет-ресурси та архітектуру Інтернету речей.
Як можна користуватися набутими знаннями і уміннями?	Здатності ініціювати, планувати та реалізовувати процеси розробки інформаційних та комп’ютерних систем та програмного забезпечення, включно з його розробкою, аналізом, тестуванням, системною інтеграцією, впровадженням і супроводом. Забезпечувати захист інформації в інформаційно-комунікаційних системах та кіберзахист об’єктів критичної інфраструктури, використовувати сучасні методології моделювання систем управління інформаційною безпекою, фреймворки управління ризиками інформаційної безпеки та кібербезпеки.
Інформаційне забезпечення дисципліни	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали
Вид семестрового контролю	Залік

Фреймворки управління ризиками інформаційної безпеки

Кафедра, яка забезпечує викладання	Спеціальна кафедра № 5.
Рівень вищої освіти	Другий (магістерський).
Курс, семестр	1 курс, весняний (2) семестр.
Обсяг дисципліни та розподіл годин	5 кредитів ЄКТС (150 годин), 72 години аудиторної роботи, 78 годин самостійної роботи.
Мова викладання	Українська, англійська.
Вимоги до початку вивчення	Для освоєння дисципліни здобувач повинен мати компетенції, отримані в результаті освоєння таких дисциплін як: “Сучасні технології програмування”, “Адміністрування та захист систем управління базами даних”, “Забезпечення якості та реверс-інжиніринг програмного забезпечення”.
Що буде вивчатися?	Ризик-орієнтований підхід до забезпечення інформаційної безпеки. Фреймворк управління ризиками інформаційної безпеки: Міжнародної організації зі стандартизації (ISO); Національного інституту стандартів і технологій (NIST); Федерального відомства з інформаційної безпеки (BSI). Фреймворк управління ризиками: кібербезпеки, ризиками безпеки програмних за стосунків; безпеки комп’ютерних мереж; безпеки ланцюгів постачання. Фреймворк управління новими ризиками інформаційної безпеки. Зокрема використання штучного інтелекту. Цикл розвідування нових ризиків для підвищення стійкості (резильєнтності) організації.
Чому це цікаво / треба вивчати?	Одним з основних завдань розроблення програмних застосунків, комп’ютерних, інформаційно-комунікаційних, інформаційно-управляючих систем та мереж є формулювання нефункційних вимог, зокрема, забезпечення безпеки. Це досягається завдяки оцінюванню ризиків інформаційної безпеки. За його результатами приймається рішення про необхідність їх обробляння і, як наслідок обираються відповідні заходи та засоби..
Чому можна навчитися?	Проєктувати архітектурні рішення інформаційних та комп’ютерних систем різного призначення. Оцінювати та забезпечувати якість інформаційних та комп’ютерних систем різного призначення. Збирати, формалізувати, систематизувати і аналізувати потреби та вимоги до інформаційної або комп’ютерної системи, що розробляється, експлуатується чи супроводжується. Створювати та досліджувати інформаційні та математичні моделі систем і процесів, що досліджуються, зокрема об’єктів автоматизації. Моделювати системи управління інформаційною безпекою, формулювати та аналізувати вимоги зацікавлених сторін до них оцінюванням і обробленням ризиків, визначати та аналізувати їхні функції, синтезувати їхню архітектуру та поведінку відповідно до сформульованих вимог зацікавлених сторін.
Як можна користуватися набутими знаннями і уміннями?	Здатність розробляти, описувати, аналізувати та оптимізувати архітектурні рішення інформаційних та комп’ютерних систем різного призначення. Здатність оцінювати та забезпечувати якість ІТ-проєктів, інформаційних та комп’ютерних систем різного призначення, застосовувати міжнародні стандарти оцінки якості програмного забезпечення інформаційних та комп’ютерних систем, моделі оцінки зрілості процесів розробки інформаційних та комп’ютерних систем. Здатність забезпечувати захист інформації в інформаційних, електронних комунікаційних, інформаційно-комунікаційних системах та кіберзахист об’єктів критичної інфраструктури, використовувати сучасні методології моделювання систем управління інформаційною безпекою, фреймворки управління ризиками інформаційної безпеки та кібербезпеки.
Інформаційне забезпечення дисципліни	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали
Вид семестрового контролю	Залік

Математичні методи побудови та аналізу асиметричних криптосистем	
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 1
Рівень вищої освіти	Другий (магістерський).
Курс, семестр	1 курс, весняний (2) семестр.
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	4 кредитів ЄКТС (120 годин), 60 години аудиторної роботи, 60 годин самостійної роботи.
Мова викладання	Українська, англійська.
Вимоги до початку вивчення	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.
Чому можна навчитися?	Застосування асиметричних алгоритмів шифрування у всіх сучасних інформаційно-комунікаційних системах.
Як можна користуватися набутими знаннями і уміннями?	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.
Інформаційне забезпечення дисципліни	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали
Вид семестрового контролю	Залік

Планування та проектування транспортних спеціальних систем електронних комунікацій

Кафедра, яка забезпечує викладання	Спеціальна кафедра № 3
Рівень вищої освіти	Другий (магістерський).
Курс, семестр	1 курс, весняний (2) семестр.
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	4 кредитів ЄКТС (120 годин), 60 години аудиторної роботи, 60 годин самостійної роботи.
Мова викладання	Українська, англійська.
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: імітаційне моделювання систем спеціального зв'язку та моніторинг і управління спеціальними інформаційно-комунікаційними системами.
Що буде вивчатися?	Основні положення теорії статистичних рішень, статистичної теорії демодуляції цифрових сигналів, на прикладах оптимального (за наявності часу – також і лінійного) розділяння 2-3-х та в деяких випадках і більшої кількості взаємно заважаючих цифрових сигналів, ознайомитись з основами теорії багатокористувацького детектування. Для найбільш підготовлених здобувачів припускається розглянути питання комплексирування протоколів ВМД і процедур РКФР за єдиним критерієм – максимуму пропускної спроможності за К. Шенноном або за А.Я. Хінчиним. Аналіз основних характеристик протоколів ВМД за додаткового припущення про розв'язання конфліктів на фізичному рівні (РКФР) і ознайомитись на прикладах з можливостями комплексування підходів, на яких базуються зазначені відгалуження в рамках загальної теорії зв'язку.
Чому це цікаво / треба вивчати?	Дає можливість розв'язувати нагальні та оригінальні задачі у сфері спеціальних систем електронних комунікацій.
Чому можна навчитися?	✓ виконувати синтез алгоритмів розділення взаємно заважаючих ЦС довільних видів та кратностей модуляції (розв'язувати задачі синтезу) за заданими критеріями переваги та проводити асимптотичний та точний аналіз їх завадостійкості; ✓ виконувати асимптотичний аналіз протоколів ВМД, комплексованих з алгоритмами БКД, включаючи додаткові припущення про розв'язання конфліктів на фізичному рівні (в демодуляторах приймальних пристроїв).
Як можна користуватися набутими знаннями і уміннями?	Застосовувати під час наукових досліджень та у процесі розв'язання часткових оптимізаційних і аналітичних задач у сфері спеціальних систем електронних комунікацій.
Інформаційне забезпечення дисципліни	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали
Вид семестрового контролю	Залік

Моделювання систем управління інформаційною безпекою

Кафедра, яка забезпечує викладання	Спеціальна кафедра № 5.
Рівень вищої освіти	Другий (магістерський).
Курс, семестр	1 курс, весняний (2) семестр.
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	4 кредитів ЄКТС (120 годин), 60 години аудиторної роботи, 60 годин самостійної роботи.
Мова викладання	Українська, англійська.
Вимоги до початку вивчення	Для освоєння дисципліни здобувач повинен мати компетенції, отримані в результаті освоєння таких дисциплін як: “Сучасні технології програмування”, “Адміністрування та захист систем управління базами даних”, “Забезпечення якості та реверс-інжиніринг програмного забезпечення”.
Що буде вивчатися?	Комплаєнс побудови та аспекти моделювання систем управління інформаційною безпекою. Ризик-орієнтований підхід до управління інформаційною безпекою. Моделе-орієнтований підхід до побудови систем управління інформаційною безпекою. Моделювання функційності, архітектури, поведінки систем управління інформаційною безпекою. Оцінювання якості систем управління інформаційною безпекою.
Чому це цікаво / треба вивчати?	Діяльність будь-якої організації обумовлюється обробленням інформації. Для цього використовуються відповідні програмні застосунки, комп’ютерні, інформаційно-комунікаційні, інформаційно-управляючі системи та мережі. Запорукою безпечності їх використання як важливих інформаційних активів є упровадження в організації проактивного заходу зі розроблення систем управління інформаційною безпекою.
Чому можна навчитися?	Проєктувати архітектурні рішення інформаційних та комп’ютерних систем різного призначення. Оцінювати та забезпечувати якість інформаційних та комп’ютерних систем різного призначення. Збирати, формалізувати, систематизувати і аналізувати потреби та вимоги до інформаційної або комп’ютерної системи, що розробляється, експлуатується чи супроводжується. Створювати та досліджувати інформаційні та математичні моделі систем і процесів, що досліджуються, зокрема об’єктів автоматизації. Моделювати системи управління інформаційною безпекою, формулювати та аналізувати вимоги зацікавлених сторін до них оцінюванням і обробленням ризиків, визначати та аналізувати їхні функції, синтезувати їхню архітектуру та поведінку відповідно до сформульованих вимог зацікавлених сторін.
Як можна користуватися набутими знаннями і уміннями?	Отримані результати навчання дозволять: розробляти, описувати, аналізувати та оптимізувати архітектурні рішення інформаційних та комп’ютерних систем різного призначення; оцінювати та забезпечувати якість ІТ-проєктів, інформаційних та комп’ютерних систем різного призначення, застосовувати міжнародні стандарти оцінки якості програмного забезпечення інформаційних та комп’ютерних систем, моделі оцінки зрілості процесів розробки інформаційних та комп’ютерних систем; ініціювати, планувати та реалізовувати процеси розробки інформаційних та комп’ютерних систем та програмного забезпечення, включно з його розробкою, аналізом, тестуванням, системною інтеграцією, впровадженням і супроводом; забезпечувати захист інформації в інформаційних, електронних комунікаційних, інформаційно-комунікаційних системах та кіберзахист об’єктів критичної інфраструктури, використовувати сучасні методології моделювання систем управління інформаційною безпекою, фреймворки управління ризиками інформаційної безпеки та кібербезпеки.
Інформаційне забезпечення дисципліни	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 (2) семестр.
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	4 кредитів ЄКТС (120 годин), 60 години аудиторної роботи, 60 годин самостійної роботи.
Мова викладання	Українська, англійська.
Вимоги до початку вивчення	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?	Основи 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?	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?	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; досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах.
Інформаційне забезпечення дисципліни	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали
Вид семестрового контролю	Залік

Сучасні інформаційні технології передачі даних в інформаційних системах

Кафедра, яка забезпечує викладання	Спеціальна кафедра № 3
Рівень вищої освіти	Другий (магістерський).
Курс, семестр	1 курс, весняний (2) семестр.
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	4 кредитів ЄКТС (120 годин), 60 години аудиторної роботи, 60 годин самостійної роботи.
Мова викладання	Українська, англійська.
Вимоги до початку вивчення	Для освоєння дисципліни здобувач повинен мати компетенції, отримані в результаті освоєння таких дисциплін як: “Сучасні технології програмування”, “Адміністрування та захист систем управління базами даних”
Що буде вивчатися?	Предметом навчальної дисципліни є сучасні проводові системи передачі, обладнання IP-телефонії, пристрої комутації та маршрутизації, основні їх технічні характеристики, принципи побудови та порядок експлуатації.
Чому це цікаво / треба вивчати?	Дає можливість розв’язувати нагальні та оригінальні задачі у сфері спеціальних систем електронних комунікацій.
Чому можна навчитися?	Здатність аналізувати стан та динамку функціонування електронних комунікаційних систем та мереж спеціального призначення, контролю та діагностики, керування якістю електронних комунікаційних послуг, метрологічного та нормативного забезпечення, стандартизації та сертифікації з використанням сучасних наукових методів і засобів аналізу, синтезу та оптимізації. Здатність до постановки та проведення наукових досліджень на відповідному рівні при вирішенні завдань з розробки та функціонування елементів транспортної платформи, мультисервісної платформи та Центру управління Національною мережею електронних комунікацій.
Як можна користуватися набутими знаннями і уміннями?	Виконувати аналіз внутрішнього та зовнішнього середовища, використовувати методи та принципи менеджменту для прийняття управлінських рішень. Орієнтувати свою службову (професійну) діяльність на розв’язання актуальних задач у сфері спеціальних систем електронних комунікацій. Формувати і постійно застосовувати системне мислення при оволодінні професією і в практичній діяльності. Працювати з науковою, науково-технічною літературою та науковою періодикою, захищати результати науково-дослідних робіт як об’єкти інтелектуальної власності, готувати звіти за результатами науково-дослідних робіт. Самостійно працювати із науковою та технічною літературою.
Інформаційне забезпечення дисципліни	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали
Вид семестрового контролю	Залік

Математичне моделювання процесів та систем	
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 5
Рівень вищої освіти	Другий (магістерський).
Курс, семестр	1 курс, весняний (2) семестр.
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	4 кредитів ЄКТС (120 годин), 60 години аудиторної роботи, 60 годин самостійної роботи.
Мова викладання	Українська, англійська.
Вимоги до початку вивчення	Для освоєння навчальної дисципліни здобувач повинен мати компетенції, отримані в результати освоєння таких навчальних дисциплін, як: імітаційне моделювання систем спеціального зв'язку; моніторинг та управління спеціальними інформаційно-комунікаційними системами.
Що буде вивчатися?	Методи і прийоми математичного та комп'ютерного моделювання процесів і систем в радіотехніці спеціального призначення.
Чому це цікаво / треба вивчати?	Дає можливість розв'язувати нагальні та оригінальні задачі у сфері спеціальних систем електронних комунікацій
Чому можна навчитися?	Застосовувати під час наукових досліджень та у процесі розв'язання часткових оптимізаційних і аналітичних задач у сфері спеціальних систем електронних комунікацій.
Як можна користуватися набутими знаннями і уміннями?	Застосовувати під час наукових досліджень та у процесі розв'язання часткових оптимізаційних і аналітичних задач у сфері спеціальних систем електронних комунікацій.
Інформаційне забезпечення дисципліни	Робоча програма навчальної дисципліни (Силабус), навчально-методичні матеріали
Вид семестрового контролю	Залік