ОПИСИ ВИБІРКОВИХ НАВЧАЛЬНИХ ДИСЦИПЛІН

за ОПП «Безпека державних інформаційних ресурсів» (магістр)

ПВ1

Назва навчальної дисципліни	**Математичні методи побудови та аналізу асиметричних криптосистем**
Рівень ВО	Другий (магістерський) рівень
Рік підготовки, семестр	І рік підготовки, весняний семестр
Обсяг	4 кредити
Мова викладання	Українська
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 1
Вимоги до початку вивчення	Успішне вирішення завдань навчальної дисципліни базується на засвоєні здобувачами знань та умінь, сформованих у них, в результаті вивчення навчальної дисципліни “Математичні методи побудови та аналізу симетричних криптосистем”. Цей курс забезпечує професійне спрямування процесу навчання здобувачів та отримання ними нових знань та навичок.
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. Метою навчальної дисципліни є формування у курсантів теоретичних знань та практичних вмінь, які необхідні для виконання обов'язків на посадах у частинах та підрозділах, що займаються проектуванням, розробкою, сертифікацією та ліцензуванням засобів криптографічного захисту інформації в автоматизованих системах, підготувати курсантів до самостійного освоєння сучасних та перспективних технологій аналізу та синтезу асиметричних криптосистем.
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 (результати навчання)	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; (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; (РН4) застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки; (РН6) аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення;

	(РН13) 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; (РН20) ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик; (РН22) 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; (РН26) 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 (компетентності)	Застосовувати під час фахової роботи в підрозділах Держспецзв'язку, які займаються проектуванням, розробкою, сертифікацією та ліцензуванням засобів криптографічного захисту інформації в автоматизованих системах.
Інформаційне забезпечення	Робоча програма навчальної дисципліни (силабус), РСО, навчально-методичні матеріали.
Форма проведення занять	Лекції, практичні заняття.
Семестровий контроль	Залік, модульна контрольна робота.

ПВ1

Назва навчальної дисципліни	**АНАЛІЗ БІНАРНИХ ВРАЗЛИВОСТЕЙ**
Рівень ВО	Другий (магістерський) рівень
Рік підготовки, семестр	І рік підготовки, весняний семестр
Обсяг	4 кредити
Мова викладання	Українська
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 1
Вимоги до початку вивчення	Успішне вирішення завдань навчальної дисципліни базується на засвоєні здобувачами знань та умінь, сформованих у них, в результаті вивчення таких навчальних дисциплін: “Технології виявлення та блокування загроз державним інформаційним ресурсам в інформаційно-комунікаційних системах” та “Автоматизація проектування цифрових пристроїв”, “Математичні методи оптимізації”. Цей курс забезпечує професійне спрямування процесу навчання здобувачів та отримання ними нових знань та навичок.
Що буде вивчатися	Предметом навчальної дисципліни є бінарні вразливості систем, що в результаті можуть призвести до проблем безпеки, таких як виконання коду, крадіжка даних або компрометація системи. Метою навчальної дисципліни є формування у курсантів теоретичних знань та практичних вмінь, які необхідні для виконання обов'язків на посадах у частинах та підрозділах, що займаються накопиченням, проведенням аналізу даних та реагуванням на кіберінциденти.
Чому це цікаво/треба вивчати	Бінарні вразливості це вразливості безпеки, виявлені в двійкових виконуваних файлах, бібліотеках або об'єктному коді. Ці вразливості можуть бути викликані різними факторами, включаючи помилки програмування, пошкодження пам'яті, помилки форматування рядків, переповнення буфера на основі стека тощо. Аналіз вразливостей націлений на попереднє виявлення та усунення причин появи загроз, аніж виявлення та блокування атак.
Чому можна навчитися (результати навчання)	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; (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; (РН4) застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки; (РН6) аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення; (РН12) 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; (РН20) ставити та вирішувати складні інженерно-

	прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик; (РН22) 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; (РН23) обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації; (РН24) 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 (компетентності)	Застосовувати під час фахової роботи в підрозділах Держспецзв'язку, які займаються накопиченням, проведенням аналізу даних та реагуванням на кіберінциденти.
Інформаційне забезпечення	Робоча програма навчальної дисципліни (силабус), РСО, навчально-методичні матеріали.
Форма проведення занять	Лекції, комп'ютерні практикуми.
Семестровий контроль	Залік, модульна контрольна робота.

ПВ2

Назва навчальної дисципліни	**Основи наукових досліджень**
Рівень ВО	Другий (магістерський) рівень
Рік підготовки, семестр	І рік підготовки, весняний семестр
Обсяг	5 кредитів
Мова викладання	Українська
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 4
Вимоги до початку вивчення	Успішне вирішення завдань навчальної дисципліни базується на засвоєні здобувачами знань та умінь, сформованих у них, в результаті вивчення таких навчальних дисциплін: “Філософія науки та інновації”, “Технології виявлення та блокування загроз державним інформаційним ресурсам в інформаційно-комунікаційних системах”, “Математичні методи побудови та аналізу симетричних криптосистем”, “Математичні методи оптимізації”, “Математичне моделювання процесів та систем” та ін., цей курс забезпечує професійне спрямування процесу навчання здобувачів та отримання ними нових знань та навичок.
Що буде вивчатися	**Метою навчальної дисципліни** є формування у курсантів наступних компетентностей: (ЗК 01) Здатність до абстрактного мислення, аналізу і синтезу; (ЗК 02) Здатність застосовувати знання у практичних ситуаціях; (ЗК 03) Здатність спілкуватися державною мовою як усно, так і письмово; (ЗК 05) Здатність вчитися й оволодівати сучасними знаннями; (ЗК 07) Здатність генерувати нові ідеї (креативність). **Предметом навчальної дисципліни** “Філософія науки та інновації” 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 (результати навчання)	Програмні результати навчання, на формування та покращення яких спрямована дисципліна: (РН3) Провадити дослідницьку та інноваційну діяльність в сфері інформаційної безпеки або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі; (РН9) Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та кібербезпекою організації на базі стратегії і політики інформаційної безпеки; (РН14) Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, операційних процесів у сфері інформаційної та кібербезпеки в цілому; (РН15) 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; (РН 16) Виконувати дослідження у сфері комп’ютерних наук; (РН 19) Аналізувати сучасний стан і світові тенденції розвитку комп’ютерних наук та інформаційних технологій. (РН25) Оцінювати

	ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.
Як можна користуватися набутими знаннями і уміннями (компетентності)	Застосовувати під час фахової та виховній роботі з особовим складом підрозділу Держспецзв'язку. Аналізувати сучасний стан і світові тенденції розвитку комп'ютерних наук, інформаційних технологій та виконувати наукові дослідження з предметної області.
Інформаційне забезпечення	Робоча програма навчальної дисципліни (силабус), РСО, навчально-методичні матеріали
Форма проведення занять	Лекції, практичні/семінарські заняття
Семестровий контроль	Залік, модульна контрольна робота

ПВ2

Назва навчальної дисципліни	**Менеджмент інформаційної безпеки держави**
Рівень ВО	Другий (магістерський) рівень
Рік підготовки, семестр	І рік підготовки, весняний семестр
Обсяг	5 кредитів
Мова викладання	Українська
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 4
Вимоги до початку вивчення	Успішне вирішення завдань навчальної дисципліни базується на засвоєні здобувачами знань та умінь, сформованих у них, в результаті вивчення таких навчальних дисциплін: “Філософія науки та інновації”, “Технології виявлення та блокування загроз державним інформаційним ресурсам в інформаційно-комунікаційних системах”, “Математичні методи побудови та аналізу симетричних криптосистем”, “Математичні методи оптимізації”, “Математичне моделювання процесів та систем” та ін., цей курс забезпечує професійне спрямування процесу навчання здобувачів та отримання ними нових знань та навичок.
Що буде вивчатися	Метою навчальної дисципліни є формування у курсантів наступних компетентностей: (КЗ-1) Здатність застосувати знання у практичних ситуаціях; (КЗ-2) Здатність проводити дослідження на відповідному рівні, застосувати знання у практичних ситуаціях; (КЗ-3) Здатність до абстрактного мислення, аналізу і синтезу. Предметом навчальної дисципліни є дотримання інформаційної безпеки держави що функціонує, а також система 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 (результати навчання)	Програмні результати навчання, на формування та покращення яких спрямована дисципліна: (РН3) Провадити дослідницьку та інноваційну діяльність в сфері інформаційної безпеки або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі; (РН9) Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та кібербезпекою організації на базі стратегії і політики інформаційної безпеки; (РН14) Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, операційних процесів у сфері інформаційної та кібербезпеки в цілому; (РН15) 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; (РН25) Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.
Як можна користуватися набутими знаннями і	Застосовувати під час фахової та виховній роботі з особовим складом підрозділу Держспецзв’язку.

уміннями (компетентності)	
Інформаційне забезпечення	Робоча програма навчальної дисципліни (силабус), РСО, навчально-методичні матеріали
Форма проведення занять	Лекції, практичні/семінарські заняття
Семестровий контроль	Залік, модульна контрольна робота

ПВ2

Назва навчальної дисципліни	**Менеджмент захисту інформаційного простору держави**
Рівень ВО	Другий (магістерський) рівень
Рік підготовки, семестр	І рік підготовки, весняний семестр
Обсяг	5 кредитів
Мова викладання	Українська
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 4
Вимоги до початку вивчення	Успішне вирішення завдань навчальної дисципліни базується на засвоєні здобувачами знань та умінь, сформованих у них, в результаті вивчення таких навчальних дисциплін: “Філософія науки та інновації”, “Технології виявлення та блокування загроз державним інформаційним ресурсам в інформаційно-комунікаційних системах”, “Математичні методи побудови та аналізу симетричних криптосистем”, “Математичні методи оптимізації”, “Математичне моделювання процесів та систем” та ін., цей курс забезпечує професійне спрямування процесу навчання здобувачів та отримання ними нових знань та навичок.
Що буде вивчатися	Метою навчальної дисципліни є формування у курсантів наступних компетентностей: (КЗ-1) Здатність застосувати знання у практичних ситуаціях; (КЗ-2) Здатність проводити дослідження на відповідному рівні, застосувати знання у практичних ситуаціях; (КЗ-3) Здатність до абстрактного мислення, аналізу і синтезу. 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 (результати навчання)	Програмні результати навчання, на формування та покращення яких спрямована дисципліна: (РН3) Провадити дослідницьку та інноваційну діяльність в сфері інформаційної безпеки або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі; (РН9) Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та кібербезпекою організації на базі стратегії і політики інформаційної безпеки; (РН14) Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, операційних процесів у сфері інформаційної та кібербезпеки в цілому; (РН15) 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; (РН25) Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.
Як можна користуватися набутими знаннями і уміннями (компетентності)	Застосовувати під час фахової та виховній роботі з особовим складом підрозділу Держспецзв’язку.

Інформаційне забезпечення	Робоча програма навчальної дисципліни (силабус), РСО, навчально-методичні матеріали
Форма проведення занять	Лекції, практичні/семінарські заняття
Семестровий контроль	Залік, модульна контрольна робота

ПВ3

Назва навчальної дисципліни	**ПРИКЛАДНА КРИПТОГРАФІЯ**
Рівень ВО	Другий (магістерський)
Рік підготовки, семестр	І рік підготовки, весняний семестр
Обсяг	3 кредити
Мова викладання	Українська
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 1
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: “Математичні методи побудови та аналізу симетричних криптосистем”, “Математичні методи побудови та аналізу асиметричних криптосистем”, цей курс забезпечує професійне спрямування процесу навчання здобувачів та проведення курсантами досліджень протягом роботи над магістерською дисертацією та переддипломної практики.
Що буде вивчатися	Предмет навчальної дисципліни є застосування криптографічних методів та алгоритмів для забезпечення послуг інформаційної безпеки. Мета навчальної дисципліни полягає в тому, щоб надати курсантам теоретичні знання та практичні навики, які необхідні для виконання обов'язків на інженерних посадах у частинах та підрозділах, що займаються проектуванням, розробкою, аналізом та застосуванням сучасних криптографічних протоколів, а також у підготовці їх до подальшого самостійного освоєння перспективних методів криптографічного захисту інформації в інформаційно-комунікаційних системах. Зміст навчальної дисципліни: сучасні стандарти у галузі криптографічного захисту інформації; основні схеми цифрового підпису та хешування; алгоритми аутентифікації; алгоритми передачі та розподілення ключів; безпека інформації на прикладному рівні.
Чому це цікаво/треба вивчати	Вивчення криптографічних методів та алгоритмів є важливою і невід'ємною складовою сучасної інформаційної безпеки. Дослідження цих протоколів дозволяє створювати та аналізувати безпечні системи, які запобігають несанкціонованому доступу до даних та захищають їх від несанкціонованих змін.
Чому можна навчитися (результати навчання)	Згідно з вимогами освітньо-професійної програми курсанти після засвоєння навчальної дисципліни мають продемонструвати такі результати навчання: - провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі; - 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; - використовувати спеціалізовані знання в області криптології, набуті у

	процесі навчання та/або професійної діяльності на рівні новітніх досягнень; - організовувати діяльність з організації робіт з проведення сертифікації засобів криптографічного захисту інформації, державної експертизи у сфері криптографічного захисту інформації, тематичних досліджень та допуску до експлуатації засобів криптографічного захисту інформації; - застосовувати методи криптографії, при вирішенні задач захисту інформації; здійснювати програмну реалізацію криптографічних алгоритмів; 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 (компетентності)	- здатність застосовувати знання у практичних ситуаціях; - здатність до абстрактного мислення, аналізу та синтезу; - 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 проводити контрольні перевірки працездатності та ефективності програмно-апаратних, криптографічних та технічних засобів захисту інформації; - здатність до систематичного вивчення та аналізу науково-технічної інформації, вітчизняного та міжнародного досвіду з криптографічного захисту інформації, брати участь у роботах з виконаних завдань та складання наукових звітів з дослідження стійкості існуючих та перспективних криптосистем та криптоалгоритмів, доцільності застосування, впровадження результатів досліджень в системах захисту інформації.
Інформаційне забезпечення	Робоча програма навчальної дисципліни (силабус), РСО, навчально-методичні матеріали.
Форма проведення занять	Лекції, практичні/семінарські заняття.
Семестровий контроль	Залік, модульна контрольна робота.

ПВ3

Назва навчальної дисципліни	**КРИПТОГРАФІЧНІ ПРОТОКОЛИ**
Рівень ВО	Другий (магістерський)
Рік підготовки, семестр	І рік підготовки, весняний семестр
Обсяг	3 кредити
Мова викладання	Українська
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 1
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: “Математичні методи побудови та аналізу симетричних криптосистем”, “Математичні методи побудови та аналізу асиметричних криптосистем”, цей курс забезпечує професійне спрямування процесу навчання здобувачів та проведення курсантами досліджень протягом роботи над магістерською дисертацією та переддипломної практики.
Що буде вивчатися	Предмет навчальної дисципліни є застосування криптографічних протоколів для забезпечення послуг інформаційної безпеки. Мета навчальної дисципліни полягає в тому, щоб надати курсантам теоретичні знання та практичні навики, які необхідні для виконання обов'язків на інженерних посадах у частинах та підрозділах, що займаються проектуванням, розробкою, аналізом та застосуванням сучасних криптографічних протоколів, а також у підготовці їх до подальшого самостійного освоєння перспективних методів криптографічного захисту інформації в інформаційно-комунікаційних системах. 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 (результати навчання)	Згідно з вимогами освітньо-професійної програми курсанти після засвоєння навчальної дисципліни мають продемонструвати такі результати навчання: - провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі; - 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;

	- використовувати спеціалізовані знання в області криптології, набуті у процесі навчання та/або професійної діяльності на рівні новітніх досягнень; - організовувати діяльність з організації робіт з проведення сертифікації засобів криптографічного захисту інформації, державної експертизи у сфері криптографічного захисту інформації, тематичних досліджень та допуску до експлуатації засобів криптографічного захисту інформації; - застосовувати методи криптографії, при вирішенні задач захисту інформації; здійснювати програмну реалізацію криптографічних алгоритмів; 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 (компетентності)	- здатність застосовувати знання у практичних ситуаціях; - здатність до абстрактного мислення, аналізу та синтезу; - 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 проводити контрольні перевірки працездатності та ефективності програмно-апаратних, криптографічних та технічних засобів захисту інформації; - здатність до систематичного вивчення та аналізу науково-технічної інформації, вітчизняного та міжнародного досвіду з криптографічного захисту інформації, брати участь у роботах з виконаних завдань та складання наукових звітів з дослідження стійкості існуючих та перспективних криптосистем та криптоалгоритмів, доцільності застосування, впровадження результатів досліджень в системах захисту інформації.
Інформаційне забезпечення	Робоча програма навчальної дисципліни (силабус), РСО, навчально-методичні матеріали.
Форма проведення занять	Лекції, практичні/семінарські заняття.
Семестровий контроль	Залік, модульна контрольна робота.

ПВ4

Назва навчальної дисципліни	**Кіберзахист об’єктів критичної інфраструктури**
Рівень ВО	Другий (магістерський) рівень
Рік підготовки, семестр	І рік підготовки, весняний семестр
Обсяг	V кредитів
Мова викладання	Українська
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 1
Вимоги до початку вивчення	Успішне вирішення завдань навчальної дисципліни “Кіберзахист об’єктів критичної інфраструктури” базується на засвоєні курсантами знань та умінь, сформованих у них, в результаті підготовки за ступенем вищої освіти бакалавр. Навчальна дисципліна забезпечує “Кібернавчання”, а також виконання магістерської дисертації.
Що буде вивчатися	Метою навчальної дисципліни є формування у курсантів наступних компетентностей: (КЗ-1) здатність застосовувати знання у практичних ситуаціях; (КЗ-2) здатність проводити дослідження на відповідному рівні; (КЗ-5) здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності); (КФ-3) здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури; (КФ-4) 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; (КФ-5) здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації; (КФ-7) 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; (КФ-9) 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; (КФ-11) здатність реалізовувати технічні вимоги на основі технік оцінки рівня захищеності інформаційних систем, технологій аналізу мережевого трафіку та принципів протидії кібератакам (КФ-11). Предметом навчальної дисципліни є системи виявлення вторгнень та системи захисту державних інформаційних ресурсі.
Чому це цікаво/треба вивчати	Дає можливість комплексного застосування підходів до захисту інформаційної інфраструктури об’єктів критичної інфраструктури, а також основних принципів категоріювання та побудови систем кіберзахисту.

Чому можна навчитися (результати навчання)	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; (РН8) Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури; (РН9) Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки; (РН10) Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації; (РН11) Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації; (РН12) 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; (РН14) Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\абокібербезпеки в цілому; (РН21) Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки; (РН24) 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 (компетентності)	Застосовувати під час фахової роботі з особовим складом підрозділу Держспецзв'язку.
Інформаційне забезпечення	Робоча програма навчальної дисципліни (силабус), РСО, навчально-методичні матеріали
Форма проведення занять	Лекції, практичні заняття
Семестровий контроль	Залік, модульна контрольна робота

ПВ4

Назва навчальної дисципліни	**Системи кібербезпеки**
Рівень ВО	Другий (магістерський) рівень
Рік підготовки, семестр	І рік підготовки, весняний семестр
Обсяг	V кредитів
Мова викладання	Українська
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 1
Вимоги до початку вивчення	Успішне вирішення завдань навчальної дисципліни “Системи кібербезпеки” базується на засвоєні курсантами знань та умінь, сформованих у них, в результаті підготовки за ступенем вищої освіти бакалавр. Навчальна дисципліна забезпечує “Кібернавчання”, а також виконання магістерської дисертації.
Що буде вивчатися	Метою навчальної дисципліни є формування у курсантів наступних компетентностей: (КЗ-1) здатність застосовувати знання у практичних ситуаціях; (КЗ-2) здатність проводити дослідження на відповідному рівні; (КЗ-5) здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності); (КФ-3) здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури; (КФ-4) 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; (КФ-5) здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації; (КФ-7) 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; (КФ-9) 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; (КФ-11) здатність реалізовувати технічні вимоги на основі технік оцінки рівня захищеності інформаційних систем, технологій аналізу мережевого трафіку та принципів протидії кібератакам (КФ-11). Предметом навчальної дисципліни є системи управління інцидентами та подіями інформаційної безпеки та системи захисту державних інформаційних ресурсів.
Чому це цікаво/треба вивчати	Дає можливість комплексного застосування підходів до захисту інформації та програмного забезпечення, знань принципів і засобів захисту інформації

	в операційних системах та комп'ютерних мережах, а також основних принципів побудови та функціонування систем забезпечення кібербезпеки.
Чому можна навчитися (результати навчання)	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; (РН8) Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури; (РН9) Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки; (РН10) Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації; (РН11) Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації; (РН12) 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; (РН24) 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 (компетентності)	Застосовувати під час фахової роботі з особовим складом підрозділу Держспецзв'язку.
Інформаційне забезпечення	Робоча програма навчальної дисципліни (силабус), РСО, навчально-методичні матеріали
Форма проведення занять	Лекції, практичні заняття
Семестровий контроль	Залік, модульна контрольна робота

ПВ 5

Назва навчальної дисципліни	**Технології організації та захисту державних інформаційних ресурсів**
Рівень ВО	Другий (магістерський) рівень
Рік підготовки, семестр	І рік підготовки, весняний семестр
Обсяг	5 кредитів
Мова викладання	Українська
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 1
Вимоги до початку вивчення	Успішне вирішення завдань навчальної дисципліни “Технології організації та захисту державних інформаційних ресурсів” базується на засвоєні курсантами знань та умінь, сформованих у них, в результаті підготовки за ступенем вищої освіти бакалавр, а також навчальної дисципліни “Технології виявлення та блокування загроз державним інформаційним ресурсам в інформаційно-комунікаційних системах”. Навчальна дисципліна забезпечує “Кібернавчання”, “Військове стажування”, а також виконання магістерської дисертації. Курс забезпечує професійне спрямування процесу навчання здобувачів та отримання ними нових знань та навичок.
Що буде вивчатися	Метою навчальної дисципліни є формування у курсантів наступних компетентностей: (КЗ-1) Здатність застосовувати знання у практичних ситуаціях. (КЗ-2) Здатність проводити дослідження на відповідному рівні. (КЗ-5) Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності). (КФ3) Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. (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. (КФ5) Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. (КФ7) 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. (КФ9) 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. (КФ11) Здатність реалізовувати технічні вимоги на основі технік оцінки рівня захищеності інформаційних систем, технологій аналізу мережевого трафіку та принципів протидії кібератакам.

	Предметом навчальної дисципліни є системи аналізу шкідливого програмного забезпечення.
Чому це цікаво/треба вивчати	Дає можливість застосування знань нормативної бази та діючих вимог до сучасних систем кібербезпеки, в тому числі і об'єктів критичної інфраструктури, а також проводити дослідження з забезпечення кібербезпеки державних інформаційних ресурсів, зокрема систем захисту від шкідливого програмного забезпечення та систем виявлення й блокування загроз.
Чому можна навчитися (результати навчання)	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; (РН6) Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення; (РН8) Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури; (РН9) Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки; (РН10) Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. (РН11) Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації; (РН12) 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; (РН14) Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\абокібербезпеки в цілому; (РН21) Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки; (РН24) 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 (компетентності)	Застосовувати під час виконання обов'язків в підрозділах Держспецзв'язку.
Інформаційне забезпечення	Робоча програма навчальної дисципліни (силабус), РСО, навчально-методичні матеріали
Форма проведення занять	Лекції, практичні/семінарські заняття
Семестровий контроль	Екзамен, модульна контрольна робота

ПВ5

Назва навчальної дисципліни	**Нормативно-правове забезпечення захисту державних інформаційних ресурсів**
Рівень ВО	Другий (магістерський) рівень
Рік підготовки, семестр	І рік підготовки, весняний семестр
Обсяг	V кредитів
Мова викладання	Українська
Кафедра, яка забезпечує викладання	Спеціальна кафедра № 1
Вимоги до початку вивчення	Успішне вирішення завдань навчальної дисципліни “Нормативно-правове забезпечення захисту державних інформаційних ресурсів” базується на засвоєні курсантами знань та умінь, сформованих у них, в результаті підготовки за ступенем вищої освіти бакалавр, а також навчальної дисципліни “Технології виявлення та блокування загроз державним інформаційним ресурсам в інформаційно-комунікаційних системах”. Навчальна дисципліна забезпечує “Кібернавчання”, “Військове стажування”, а також виконання магістерської дисертації. Курс забезпечує професійне спрямування процесу навчання здобувачів та отримання ними нових знань та навичок.
Що буде вивчатися	Метою навчальної дисципліни є формування у курсантів наступних компетентностей: (КЗ-1) Здатність застосовувати знання у практичних ситуаціях; (КЗ-2) Здатність проводити дослідження на відповідному рівні; (КЗ-5) Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності); (КФ3) Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури; (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; (КФ5) Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації; (КФ11) Здатність реалізовувати технічні вимоги на основі технік оцінки рівня захищеності інформаційних систем, технологій аналізу мережевого трафіку та принципів протидії кібератакам. Предметом навчальної дисципліни є системи аналізу шкідливого програмного забезпечення.
Чому це цікаво/треба вивчати	Дає можливість застосування знань нормативної бази та діючих вимог до сучасних систем захисту інформації, в тому числі і забезпечення кібербезпеки, а також створення політик безпеки на основі кращих практик та міжнародних стандартів.
Чому можна навчитися	Програмні результати навчання, на формування та покращення яких спрямована дисципліна: (РН2) Інтегрувати фундаментальні та спеціальні

(результати навчання)	знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах; (РН6) Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення; (РН8) Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури; (РН9) Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки; (РН10) Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації; (РН11) Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації; (РН14) Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\абокібербезпеки в цілому; (РН24) 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 (компетентності)	Застосовувати під час виконання обов’язків в підрозділах Держспецзв’язку.
Інформаційне забезпечення	Робоча програма навчальної дисципліни (силабус), РСО, навчально-методичні матеріали
Форма проведення занять	Лекції, практичні/семінарські заняття
Семестровий контроль	Екзамен, модульна контрольна робота