Прим. № 1

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Комплексні системи захисту інформації»

Освітня програма	Кіберзахист інформаційних ресурсів
Рівень вищої освіти	перший (бакалаврський)
Форма навчання	денна
Статус навчальної дисципліни	обов'язкова
Мова викладання	українська

КИЇВ – 2024

Робочу програму навчальної дисципліни розглянуто та затверджено на засіданні кафедри кібербезпеки ЦКБ ННІ ІБ СК НА СБ України від «02» 09 2024 року, протокол № 15.

1. Опис навчальної дисципліни

Показник	Значення показника
Курс	4
Семестр	8
Обсяг *(кредити ЄКТС/години)*	5 / 150
Кількість змістових модулів	3
Розподіл годин за видами навчальної діяльності:	
лекції (Л)	30
семінарські заняття (СЗ)	
практичні заняття (ПЗ)	44
лабораторні заняття (ЛЗ)	-
самостійна робота (СР)	76
форма підсумкового контролю *(семестр)*	екзамен (8)

2. Мета та завдання навчальної дисципліни

2.1. Мета та основні завдання вивчення навчальної дисципліни

Мета: формування у курсантів сучасного рівня інформаційної культури, набуття знань про методи і принципи побудови організаційної, програмної та технічної бази сучасних систем захисту інформації інформаційно-комунікаційних системах (ІКС), набуття знань щодо організації роботи керівника служби захисту інформації, помічника керівника підприємства (установи, організації) з питань захисту інформації.

Завдання: набуття теоретичних знань і практичних навичок щодо:

- основних понять та визначень КСЗІ, вимог законодавства та нормативних документів з технічного захисту інформації (далі – НД ТЗІ) щодо етапів життєвого циклу КСЗІ, зокрема, стосовно умов і порядку її створення та забезпечення функціонування;
- методів, засобів та заходів з захисту інформації в автоматизованих системах (АС) від несанкціонованого доступу (НСД) та витоку технічними каналами;
- порядку та правил проведення робіт зі створення КСЗІ, державного регулювання господарської діяльності у сфері криптографічного та технічного захисту інформації (далі – КЗІ та ТЗІ);
- основних підходів щодо організації обстеження об'єктів інформаційної діяльності та документального оформлення його результатів;
- принципів побудови критеріїв оцінки захищеності АС, формування (вибору) профілю захисту АС для різних видів інформації з обмеженим доступом та АС різних класів;
- порядку проведення державної експертизи у сфері КЗІ та ТЗІ,
- сутності моделі загроз, моделі порушника, плану захисту інформації в АС та основних підходів до їх розроблення;
- функцій та завдань служби захисту інформації;
- змісту етапів створення КСЗІ, випробувань і введення в експлуатацію;
- вивчення порядку проведення робіт зі створення комплексу ТЗІ,

- ознайомлення з науково-практичними дослідженнями КСЗІ;
- надбання вмінь та навичок розробки проектів нормативно-розпорядчих документів з питань захисту інформації, застосування сучасних методів та засобів захисту при вирішенні практичних завдань, пов'язаних з побудовою КСЗІ.

2.2. Результати навчання

Обов'язкова навчальна дисципліна «Комплексні системи захисту інформації» спрямована на досягнення програмних результатів навчання, які в інтегрованому (синтезованому) вигляді визначені у профілі освітньо-професійної програми «Контррозвідувальний захист кібербезпеки держави та об'єктів критичної інфраструктури» *(від 11.09.2024 № 29/3/1/3-1277/ві),* а саме:

ПРН-05	Адаптуватись до нових викликів та дій у певних ситуаціях, застосовувати знання державної та іноземних мов, інформаційно – комунікаційних технологій, комп'ютерної техніки для забезпечення професійної комунікації.
ПРН-13	Оцінювати стан безпеки особистості, суспільства та держави за окремими сферами забезпечення і видами діяльності на основі положень теорії безпеки окремих сфер забезпечення національної безпеки і видів діяльності.
ПРН-15	Аналізувати та упорядковувати основні властивості об'єктів безпеки окремих сфер забезпечення національної безпеки і видів діяльності та здійснювати класифікацію загроз об'єктам безпеки, класифікацію та ранжирування джерел загроз і уразливостей безпеки
ПРН-16	Розробляти основні положення методів та заходів забезпечення інформаційної безпеки та кібербезпеки держави у різноманітних сферах життєдіяльності.
ПРН-17	Здійснювати заходи щодо запобігання розголошення секретної інформації, випадкам втрат матеріальних носіїв цієї інформації, заволодіння цією інформацією іноземними державами, іноземними юридичними особами, іноземцями, особами без громадянства та громадянами України, яким не надано допуск та доступ до неї
ПРН-18	Обґрунтовувати побудову систем та засобів фізичного захисту та захисту від зовнішніх впливів об'єктів інформаційної інфраструктури та кіберінфраструктури.
ПРН-20	Визначати, розробляти та впроваджувати ефективні системи технічного захисту інформації на об'єктах інформаційної та кіберінфраструктури, застосовуючи сучасні технології та методи для забезпечення безпеки інформаційних ресурсів
ПРН-21	Вирішувати завдання захисту інформації, що обробляється на об'єктах інформаційної інфраструктури та кіберінфраструктури, з використанням методів, засобів і механізмів криптографічного захисту інформації, а також володіти методами сучасних систем

	цифрової криміналістики і застосовувати їх в дослідницькій та прикладній діяльності.
ПРН-24	Забезпечувати процеси захисту та функціонування інформаційно-комунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
ПРН-25	Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцидентів в сфері кібербезпеки

3. Програма та структура навчальної дисципліни

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	ЛЗ	СР
1	*2*	*3*	*4*	*5*	*6*	*7*
Семестр 8						
Модуль 1. Комплексний підхід до захисту інформації						
Тема 1. Загальні засади захисту інформації	**10**	**2**		**4**		**4**
Лекція 1. Основні поняття та визначення комплексного захисту інформації		2				
Самостійна робота 1. Опрацювання матеріалів лекції 1						4
Практичне заняття 1. Інформація як об'єкт захисту				2		
Практичне заняття 2. Понятійний апарат КЗІ та ТЗІ, інженерно-технічного захисту на ОІД				2		
Тема 2. Методи, засоби і заходи захисту інформації	**8**	**2**		**2**		**4**
Лекція 2. Методи, засоби та заходи захисту інформації в АС від НСД		2				
Самостійна робота 2. Опрацювання матеріалів лекції 2						4
Практичне заняття 3. Методи, засоби та заходи захисту інформації в АС від витоку та руйнування технічними каналами. **Модульна контрольна робота №1**				2		
Всього годин за модуль 1	**18**	**4**		**6**		**8**
Модуль 2. Проектування, введення в експлуатацію та супроводження КСЗІ						
Тема 3. Загальні засади побудови КСЗІ	**28**	**6**		**10**		**12**
Лекція 3. Порядок проведення робіт зі створення КСЗІ		2				

Самостійна робота 3. Опрацювання матеріалів лекції 3						4
Практичне заняття 4. Порядок створення, введення в експлуатацію та супроводження КСЗІ				2		
Лекція 4. Політика безпеки інформації в АС, основні підходи та принципи розроблення технічного завдання на створення КСЗІ		2				
Самостійна робота 4. Опрацювання матеріалів лекції 4						4
Практичне заняття 5. АС класу 1: Загальний опис акт обстеження, акт категоріювання				2		
Практичне заняття 6. Основні підходи та принципи розроблення плану захисту для АС класу 1				2		
Лекція 5. Введення КСЗІ в експлуатацію		2				
Самостійна робота 5. Опрацювання матеріалів лекції 3						4
Практичне заняття 7. Модель загроз, модель порушника.				2		
Практичне заняття 8. План захисту для АС класу 1				2		
Тема 4. Проєктування та експлуатація КСЗІ	**42**	**10**		**12**		**20**
Лекція 6. Принципи побудови критеріїв оцінки захищеності АС		2				
Самостійна робота 6. Опрацювання матеріалів лекції 1						4
Практичне заняття 9. Побудова критеріїв оцінки захищеності АС				2		
Лекція 7. Особливості проектування КСЗІ для АС різних класів		2				
Самостійна робота 7. Опрацювання матеріалів лекції 7						4
Практичне заняття 10. Індивідуальне завдання на АС класу 1: інструкції адміністратора безпеки і користувача, формуляр				2		
Лекція 8. Особливості захисту службової інформації від НСД в ІТС класу 2		2				
Самостійна робота 8. Опрацювання матеріалів лекції 8						4
Лекція 9. Випробування комплексу ТЗІ та його атестація		2				
Самостійна робота 9 Опрацювання матеріалів лекції 4						4
Практичне заняття 11. Адміністрування				2		

операційної системи Windows						
Лекція 10. Управління комплексною системою захисту інформації в ІТС		2				
Самостійна робота 10. Опрацювання матеріалів лекції 5						4
Практичне заняття 12. Індивідуальне завдання на АС класу 1: Програма та методика приймальних випробувань КСЗІ, акт завершення робіт.				2		
Практичне заняття 13. Побудова системи управління інформаційною безпекою				2		
Практичне заняття 14. Аудит системи управління інформаційною безпекою. **Модульна контрольна робота №2**				2		
Всього годин за модуль 2	**70**	**16**		**22**		**32**
Модуль 3. Організаційно-правові засади кіберзахисту критичної інформаційної інфраструктури						
Тема 5. Вимоги до кіберзахисту об'єктів критичної інформаційної інфраструктури	**62**	**10**		**16**		**36**
Лекція 11. Загальні засади правого регулювання захисту критичної інфраструктури		2				
Самостійна робота 11. Опрацювання матеріалів лекційного заняття 11						4
Самостійна робота 12. Опрацювання нормативно-правових джерел до практичного заняття 15						4
Практичне заняття 15. Ідентифікація та паспортизація об'єктів критичної інфраструктури				2		
Лекція 12. Реєстр об'єктів критичної інформаційної інфраструктури		2				
Самостійна робота 13. Опрацювання матеріалів лекційного заняття 12						2
Самостійна робота 14. Опрацювання нормативно-правових джерел до практичного заняття 15						2
Практичне заняття 16. Категорії критичності об'єктів критичної інфраструктури				2		
Самостійна робота 15. Опрацювання нормативно-правових джерел до практичного заняття 16						4
Практичне заняття 17. Внесення об'єктів до реєстру об'єктів критичної інформаційної інфраструктури				2		
Лекція 13. Організаційно-технічна модель		2				

кіберзахисту						
Самостійна робота 16. Опрацювання матеріалів лекційного заняття 13						4
Самостійна робота 17. Опрацювання нормативно-правових джерел до практичного заняття						4
Практичне заняття 18. Функціонування організаційно-технічної моделі кіберзахисту				2		
Самостійна робота 18. Опрацювання нормативно-правових джерел до практичного заняття 18						4
Практичне заняття 19. Досвід країн ЄС і НАТО в сфері кіберзахисту критичної інфраструктури				2		
Лекція 14. Загальні вимоги до кіберзахисту об'єктів критичної інформаційної інфраструктури		2				
Самостійна робота 19. Опрацювання матеріалів лекційного заняття 14						2
Самостійна робота 20. Опрацювання нормативно-правових джерел до практичного заняття 20						2
Практичне заняття 20. Загальна політика інформаційної безпеки на об'єкті критичної інформаційної інфраструктури				2		
Самостійна робота 21. Опрацювання нормативно-правових джерел до практичного заняття 21						
Практичне заняття 21. Реалізація заходів кіберзахисту на об'єкті критичної інформаційної інфраструктури				2		
Лекція 15. Спеціальні рекомендації щодо кіберзахисту об'єктів критичної інфраструктури		2				
Самостійна робота 22. Опрацювання матеріалів лекційного заняття 15						2
Самостійна робота 23. Опрацювання нормативно-правових джерел до практичного заняття 22						2
Практичне заняття 22. Класифікація заходів кіберзахисту. Профілі кіберзахисту об'єкта критичної інформаційної інфраструктури. Модульна контрольна робота №3				2		
Всього годин за модуль 3	**62**	**10**		**16**		**36**
Всього годин за навчальну дисципліну	**150**	**30**		**44**		**76**
Підсумковий контроль (*екзамен*)						

Організаційно-методичні вказівки до проведення навчальних занять та контрольних заходів: *планувати проведення лекційних і практичних занять в центрі кібербезпеки.*

4. Основні методи навчання

Під час викладання навчальної дисципліни передбачено застосування наступних форм.

Лекція – логічно вивершений, науково обґрунтований та систематизований виклад певного наукового або науково-педагогічного питання, ілюстрований засобами наочності та демонстрацією результатів досліджень.

Лекція є одним із основних видів і, водночас, методів проведення навчальних занять, призначених для засвоєння теоретичного матеріалу. Вона закладає основи наукових знань, визначаючи напрям, основний зміст та характер усіх видів навчальних занять, а також, головним чином, самостійної роботи здобувачів вищої освіти.

Практичне заняття – форма навчального заняття, на якому у здобувача вищої освіти під керівництвом викладача формуються вміння та навички практичного застосування теоретичних положень навчальної дисципліни шляхом виконання здобувачем вищої освіти відповідно сформульованих завдань.

Практичні заняття проводяться в аудиторії, оснащеною комп'ютерною технікою та технічними засобами навчання.

Практичне заняття включає в себе: проведення викладачем контролю знань, вмінь та навичок здобувачів вищої освіти, постановку загальної проблеми (завдання) та її обговорення за участю здобувачів вищої освіти, розв'язування завдань та їх обговорення, виконання контрольних завдань, їх перевірку та оцінювання викладачем.

Консультація – форма навчального заняття, на якому здобувач вищої освіти отримує від викладача відповіді на конкретні запитання або пояснення окремих теоретичних положень та їх використання на практиці.

Самостійна робота забезпечується навчально-методичними засобами, передбаченими для вивчення навчальної дисципліни: підручниками, навчально-методичними посібниками, конспектами лекцій, практикумами, електронно-обчислювальною технікою тощо.

Самостійна робота над засвоєнням навчального матеріалу може виконуватися в бібліотеці, комп'ютерному класі.

Форми самостійної роботи здобувачів вищої освіти:

- опрацювання теоретичних основ прослуханого лекційного матеріалу;
- вивчення окремих тем або питань, передбачених для самостійного опрацювання;
- виконання різних за формою і змістом завдань;
- підготовка до практичних занять;

- підготовка до поточного, модульного та підсумкового контролю знань;
- пошук та огляд літературних джерел за проблематикою навчальної дисципліни;
- аналітичний розгляд наукової публікації тощо.

Під час викладання навчальної дисципліни «Комплексні системи захисту інформації» використовуються такі методи навчання: індуктивний, дедуктивний, дослідницький та метод стимулювання.

Індуктивний метод полягає в тому, що викладач спершу викладає факти, проводить досліди, поступово підводить слухачів до узагальнень, визначення понять. Дедуктивний метод полягає в тому, що викладач повідомляє загальне положення, закон, а потім роблячи висновки поступово підводить до конкретних висновків, ставить конкретні завдання. Дослідницький метод пов'язаний з опануванням нових знань у процесі творчої роботи. Дослідницький метод застосовується для засвоєння досвіду творчої діяльності, глибоких знань. Методи стимулювання спеціально спрямовані на формування позитивних мотивів навчання, стимулюють пізнавальну активність, водночас сприяють збагаченню здобувачів вищої освіти новою інформацією.

Теоретична підготовка здобувачів вищої освіти забезпечується шляхом вивчення вимог керівних документів з питань національної та інформаційної безпеки, політико-правових аспектів формування інформаційного суспільства держави, науково-методичних засад державного управління національними інформаційними ресурсами як необхідної складової системи інформаційної безпеки.

Основними видами занять є лекції, практичні, семінарські та самостійні заняття.

5. Оцінювання результатів навчання

5.1 Результати навчання здобувача вищої освіти з навчальної дисципліни оцінюються за 100-бальною шкалою як сума балів поточного та підсумкового контролю із застосуванням наступних вагових коефіцієнтів, загальна сума яких дорівнює 1:

Вид контролю	Ваговий коефіцієнт
Поточний контроль (К)	**0,8**
Підсумковий контроль (ПК)	**0,2**

Підсумкова семестрова оцінка (ПСО) обчислюється за формулою: ПСО=К+ПК

5.2. Складниками для обчислення балу поточного контролю здобувача вищої освіти є:

Види навчальної діяльності	Кількість балів (максимальна)
Робота на лекціях (ведення конспекту лекцій або інше)	10
Робота на практичних заняттях	50
Виконання завдань для самостійної роботи	10
Виконання модульної контрольної роботи	10

Мінімальна кількість балів для допуску до підсумкового контролю 48 балів.

5.3. Шкала оцінювання здобувача вищої освіти

Оцінка за шкалою ЄКТС	Оцінка за 100-бальною шкалою	Значення оцінки
A	90-100	*Відмінно – відмінне виконання лише з незначною кількістю помилок.* Здобувач вищої освіти виявляє особливі творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить та опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні обдарування і нахили.
B	84-89	*Дуже добре – вище середнього рівня, але з кількома помилками.* Здобувач вищої освіти вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв'язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна
C	75-83	*Добре – загалом правильна робота, але з певною кількістю помилок.* Здобувач вищої освіти вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом викладача; в цілому самостійно застосовувати її на практиці; контролювати власну діяльність; виправляти помилки, серед яких є суттєві, добирати аргументи для підтвердження думок.
D	65-74	*Задовільно – непогано, але зі значною кількістю недоліків.*

		Здобувач вищої освіти відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень; з допомогою викладача може аналізувати навчальний матеріал, виправляти помилки, серед яких є значна кількість суттєвих.
E	60-64	*Достатньо – виконання задовольняє мінімальні вимоги.* Здобувач вищої освіти володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні.
FX	35-59	*Незадовільно – потрібна додаткова робота.* Здобувач вищої освіти володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу
F	1-34	*Незадовільно – потрібна значна додаткова робота.* Здобувач вищої освіти володіє матеріалом на рівні елементарного розпізнання і відтворення окремих фактів, елементів, об'єктів.

6. Ресурсне забезпечення навчальної дисципліни

Рекомендовані джерела інформації

Основна література:

1. Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації: підручник/ - Вінниця: ВНТУ, 2011. - 199с.

2. Мамченко С.М. Комплексні системи захисту інформації: Навч. посіб. / С.М. Мамченко, В.Д. Козюра, В.Д. Бровко. – Київ: Нац. Акад. СБУ, 2018. – 372 с. [Режим доступу]: МЕТОД/СК-31/КСЗІ/ Література

3. Гуз А.М., Довгань О.Д., Марущак А.І.: Основи захисту інформації з обмеженгим доступом: підручник/ К.: НА СБУ, 2011 р.

4. Блавацька Н.М. ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ: підручник / Н.М.Блавацька, В.Д.Козюра, В.О.Хорошко. – К.: Вид. ДУІКТ, 2011. – 330 с. [Режим доступу]: МЕТОД/СК-31/КСЗІ/ Література

2. Гулак Г.М., Гринь А.К., Довгань О.Д., Мельник С.В. Методологія захисту інформації: навчально-методичний посібник. – К.: Видавництво НА СБ України, 2013. – 184 с.

3. Бурячок В.Л., Гулак Г.М., Толубко В.Л. Інформаційний та кібернетичний простори: проблеми безпеки, методи та засоби боротьби Підручник. – К.: ТОВ «СІК ГУП Україна», 2015. – 449 с.

Допоміжна література:

1. Богуш В.М., Юдін О.К., Інформаційна безпека держави. –К.: «МК-Прес», 2005. – 432с.

2. Гайворонський М.В. БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ / М.В.Гайворонський, О.М.Новиков. - К.: Видавнича група BHV, 2009. - 608 с. [Режим доступу]: МЕТОД/СК-31/КСЗІ/ Література

3. Богуш В.М. ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ: ВСТУП ДО СПЕЦІАЛЬНОСТІ / В.М.Богуш, О.К.Юдін. – Харків: Консум, 2004. – 439 с.

Нормативно-правові акти:

1. Закон України "Про інформацію" від 02.10.1992 № 2657-XII.
2. Про державну таємницю Закон України від 21.01.1994 № 3855-XII
3. Про захист інформації в інформаційно-комунікаційних системах Закон України від 05.07.1994 № 80/94-ВР.
4. Про електронні довірчі послуги Закон України від 5.10.2017 № 2155-VIII
5. Про Національну систему конфіденційного зв'язку Закон України від 10.01.2002 № 2919-III
6. Про Державну службу спеціального зв'язку та захисту інформації України Закон України від 23.02.2006 № 3475-IV
7. Про Положення про порядок здійснення криптографічного захисту інформації в Україні Указ Президента України від 22.05.1998 № 505/98
8. Про затвердження Технічного регламенту засобів криптографічного захисту інформації. Постанова Кабінету Міністрів України від 21.10.2020 р. № 991

Інформаційні ресурси

1. Національна бібліотека ім. В.І.Вернадського / [Електронний ресурс]. – Режим доступу: http:www.nbuv.gov.ua/

2. Цифровий репозитарій ХНУГХ ім. А.Н.Бекетова / [Електронний ресурс]. – Режим доступу: http://eprints.kname.edu.ua/

3. Цифровий репозитарій Харківського національного університету ім. В.Н.Каразіна / [Електронний ресурс]. – Режим доступу: http://dspace.univer.kharkov.ua/handle/123456789/568

Адреса розміщення робочої програми навчальної дисципліни:
https://academy.ssu.gov.ua/

(офіційний вебсайт НА СБУ / платформа дистанційного навчання / електронний ресурс навчально-наукового інституту, кафедри, бібліотеки тощо)

7. Дані про перегляд робочої програми навчальної дисципліни

№ п/п	Дата, номер протоколу засідання кафедри (спільного засідання кафедр)	Рішення за результатами перегляду	Підпис керівника кафедри
1.			
2.			
3.			
4.			
5.			

29/3/1/1-1539/Кі
10.10.24