

1. Опис навчальної дисципліни

Показник	Значення показника
Курс (и)	1
Семестр (и)	1
Обсяг (<i>кредити ЄКТС/години</i>)	4 / 120
Кількість змістових модулів	2
Розподіл годин за видами навчальної діяльності:	
лекції (Л)	10
семінарські заняття (СЗ)	4
практичні заняття (ПЗ)	-
лабораторні заняття (ЛЗ)	-
індивідуальні завдання (ІЗ)	-
самостійна робота (СР)	106
форма підсумкового контролю (<i>семестр</i>)	диф. залік

Передумови для вивчення навчальної дисципліни - немає

2. Мета та завдання навчальної дисципліни

2.1. Мета – полягає у формування у студентів цілісних знань про організаційно-правові норми, які регламентують суспільні відносини в галузі управління безпекою державних і недержавних організацій та підприємств з огляду на дотримання міжнародних стандартів захисту інформації.

2.2. Завдання:

1. організації свідомого засвоєння студентами системи знань про міжнародні стандарти безпеки (ISO/IES);
2. створення повної, точної та логічної послідовності картини створення інформаційної безпеки відповідно з вимогами міжнародних безпекових стандартів;
3. стимулювання у студентів стійкого інтересу до міжнародних стандартів.

2.3. Результати навчання

Обов'язкова навчальна дисципліна «Міжнародні стандарти захисту інформації» спрямована на досягнення програмних результатів навчання, які в інтегрованому (синтезованому) вигляді визначені у профілі освітньо-

професійної програми «Організація захисту інформації з обмеженим доступом» (від __. __.202__ № __), а саме:

ПРН 2.	Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності.
ПРН 9.	Синтезувати спектр заходів та підходів, що можуть використовуватись для вирішення проблем, пов'язаних з викликами глобальній, європейській та регіональній безпеці.

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 I						
Змістовий модуль 1.						
Методологічні основи положень та коментарів до міжнародних стандартів						
Тема 1. Основні терміни та визначення. Політика безпеки. ISO/IES 17799, ISO/IES 27001, ISO/IES 17799, ISO/IES 15408		4	2			15
Лекція 1. Основні терміни та визначення. Політика безпеки. ISO/IES 17799, ISO/IES 27001, ISO/IES 17799, ISO/IES 15408		2				
Самостійна робота 1. Становлення світових стандартів інформаційної безпеки						5
Семінарське заняття 1. Розвиток світових стандартів інформаційної безпеки			2			
Самостійна робота 2. Аналіз положень стандартів ISO/IES 17799, ISO/IES 27001, ISO/IES 17799, ISO/IES 15408						5
Самостійна робота 3. Еволюція міжнародних стандартів з інформаційної безпеки						5
Тема 2. Організаційні заходи по забезпеченню безпеки. Розподіл відповідальності		2				25
Лекція 1. Організаційні заходи із забезпечення безпеки інформації НАТО		2				
Самостійна робота 1. Стандарти серії ISO 27000 «Міжнародні стандарти для системи управління інформаційною безпекою»						5
Самостійна робота 2. Стандарти серії ISO 27000 «Міжнародні стандарти для системи управління інформаційною безпекою»						5
Самостійна робота 3. Функції служби захисту інформації						5
Самостійна робота 4. Організаційні заходи по забезпеченню безпеки. Розподіл відповідальності						5
Самостійна робота 5. Стандарт ISO/IEC 17799						5
Всього годин за змістовий модуль 1.		4	2			40
Змістовий модуль 2.						
Основні положення концепції забезпечення безпеки вітчизняного підприємства в ракурсі гармонізації міжнародних стандартів безпеки з державними стандартами України						
Тема 1. Класифікація та управління ресурсами. Інвентаризація ресурсів		2	2			15
Лекція 1. Класифікація та управління ресурсами. Інвентаризація ресурсів		2				
Самостійна робота 1. Міжнародні стандарти, прийняті в Україні як національні						5
Семінарське заняття 1. Міжнародні стандарти, прийняті в Україні як національні			2			
Самостійна робота 2. Застосування міжнародних стандартів у вирішенні проблем управління інформаційною безпекою						5
Самостійна робота 3. Класифікація та управління ресурсами. Інвентаризація ресурсів						5
Тема 2. Безпека персоналу. Підбір. Тренінги. Фізична безпека		2				20
Лекція 1. Безпека персоналу, підбір, тренінги, фізична безпека		2				
Самостійна робота 1. Стандарти серії ISO 13335 «Міжнародні стандарти безпеки інформаційних технологій»						5

1	2	3	4	5	6	7
Самостійна робота 2. Стандарти серії ISO 13335 «Міжнародні стандарти безпеки інформаційних технологій»						5
Самостійна робота 3. Основні заходи забезпечення безпеки персоналу, підбору, тренінгів, фізичної безпеки						5
Самостійна робота 4. Фізичний захист і захист від впливу навколишнього середовища.						5
Тема 3. Управління комунікаціями та процесами. Контроль доступу		2				31
Лекція 1. Управління комунікаціями та процесами. Контроль доступу		2				
Самостійна робота 1. Стандарт ISO/IES 15408						8
Самостійна робота 2. Організаційні заходи із забезпечення безпеки інформації НАТО						8
Самостійна робота 3. Обґрунтування актуальності стандарту ISO/IES 15408						7
Самостійна робота 4. Політика безпеки і сутність організаційно-правових аспектів захисту інформації з обмеженим доступом в країнах НАТО та ЄС						8
Всього годин за змістовий модуль № 2		6	2			31
Підсумковий контроль (форма)	диф.залік					
Всього годин за навчальну дисципліну	120	10	4			106

4. Основні методи навчання

I. Методи організації та здійснення навчально-пізнавальної діяльності:

1. За джерелом інформації:
словесні: лекція (традиційна, проблемна) із застосуванням комп'ютерних інформаційних технологій, семінари, пояснення, розповідь, бесіда;
наочні: спостереження, ілюстрація, демонстрація.
2. За логікою передачі і сприймання навчальної інформації: індуктивні, дедуктивні, аналітичні, синтетичні.
3. За ступенем самостійності мислення: репродуктивні, пошукові, дослідницькі.
4. За ступенем керування навчальною діяльністю: під керівництвом викладача; самостійна робота студентів: з книгою; виконання індивідуальних навчальних проектів.

II. Методи стимулювання інтересу до навчання і мотивації навчально-пізнавальної діяльності:

- навчальні дискусії;
- створення ситуації пізнавальної новизни;
- створення ситуацій зацікавленості (метод цікавих аналогій тощо).

Складання конспекту з теми модуля за заданим, або самостійно складеним планом.

Підготовка доповідей з теми модуля.

Розробка тестових завдань з теми модуля.

Добір додаткового теоретичного та ілюстративного матеріалу.

Написання самостійної роботи з теми модуля.

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)	0,6
Підсумковий контроль (ПК)	0,4

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)	5
Робота на семінарських заняттях	5
Робота на практичних заняттях	5
Виконання завдань для самостійної роботи	5

Мінімальна кількість балів для допуску до підсумкового контролю – 35

5.3. Шкала оцінювання здобувача вищої освіти

Оцінка за шкалою ЄКТС	Оцінка за 100-бальною шкалою	Значення оцінки
A	90-100	<i>Відмінно – відмінне виконання лише з незначною кількістю помилок.</i> 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	<i>Дуже добре – вище середнього рівня, але з кількома помилками.</i> 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	<i>Добре – загалом правильна робота, але з певною кількістю помилок.</i> 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	<i>Задовільно – непогано, але зі значною кількістю недоліків.</i> 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	<i>Достатньо – виконання задовольняє мінімальні вимоги.</i> Здобувач вищої освіти володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні.
FX	35-59	<i>Незадовільно – потрібна додаткова робота.</i> Здобувач вищої освіти володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу
F	1-34	<i>Незадовільно – потрібна значна додаткова робота.</i> Здобувач вищої освіти володіє матеріалом на рівні елементарного розпізнання і відтворення окремих фактів, елементів, об'єктів.

6. Ресурсне забезпечення навчальної дисципліни

Основна література:

1. Ярема О.Г., Ілюшук О.М. Система правових засобів забезпечення інформаційної безпеки. Аналітично-порівняльне правознавство. №4. (2022). С. 237-241.
2. Інформаційне право : підручник / [Л. П. Коваленко, Б. В. Коваленко] ; за заг. ред. Л. П. Коваленко ; Нац. юрид. ун-т ім. Ярослава Мудрого. Одеса : Гельветика, 2020. 285 с.
3. Інформаційна безпека держави : підручник / за аг. ред.. В.В. Остроухова. Київ: ДНУ «Книжкова палата Україна», 2016. 264 с. 6. Інформаційне право : підручник / [Л. П. Коваленко, Б. В. Коваленко] ; за заг. ред. Л. П. Коваленко ; Нац. юрид. ун-т ім. Ярослава Мудрого. Одеса : Гельветика, 2020. 285 с.
4. Богданов О., Бакалинський О. «Адаптація міжнародного стандарту управління інформаційною безпекою ISO / ІЕС 27001:2005у структурах державного управління України». [Електронний ресурс]. – Режимдоступу:http://nc.nusta.com.ua/Kyrsi%202021/tezi/images_tezi/S_6_Vogdanov_Bakalynsky_1.htm

Допоміжна література:

1. Управління та організація служби захисту інформації: навч. посіб. / А.К. Гринь – К. Нац. Акад. СБУ, 2010. – 71 с.
2. Міжнародне співробітництво у сфері охорони державної таємниці: навч. посіб. / [авт. кол. Т.Ю. Ткачук, А.М. Гуз, С.О. Князев та інші] – К. : Наук.-вид. відділ НА СБ України., 2019. – 91с.

Нормативно-правові акти

1. ISO/IES 17799 Управління інформаційною безпекою – державний стандарт, УкрЦСМ, 2004 р.
2. Міжнародний стандарт ISO/IEC 27001:2005 "Системи менеджмента інформаційної безпеки. Вимоги"
3. ISO/IES 15408– державний стандарт, УкрЦСМ, 2004 р.

Інформаційні ресурси

1. C-M(2002)60, July 23, 2002, released by US OSD January 28, 2005. – <http://www.nato.int>.
2. PO(90)32(Revised), Public Disclosure of NATO Documents. February 20, 1995. Released by UK MOD to BASIC, January 2005. Alternative version released by US OSD January 28, 2005. – <http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf>.
3. NATO Research And Technical Organization Technical Publication Policy, 4th Issue – March 2001, Section VINATO/Pfp UNCLASSIFIED, AC/323-D/22. PDF from Nato website March 26, 2002. – <http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf>.
C-M(55)15(Final), Security Within the North Atlantic Treaty Organization. July 31, 1964. – <http://www.nato.int>.
Confidential Supplement to C-M(55)15(Final), 1964. – <http://nato.int.gb>.

4. Peter Sobcak, "New Security Office to Guard NATO Secrets," Slovak Army Review (Spring 2002). – <http://csrc.nist.gov/publications.pdf>.
5. The Associated Press (Bucharest, Romania), "NATO Officials Want Romania to Exclude Some Former Communists from Intelligence Positions," March 20, 2002. – <http://cio.gov/Documents/computer.html>.
6. NATO, Membership Action Plan (Brussels: NATO, April 24,1999), Press Release NAC-S(99) 66. – <http://cio.gov/Documents.html>.
7. "NATO Used as Scarecrow to Pass Law on Secrets," Bucharest Ziua (Bucharest), April 8, 2002, at. – www.ziua.ro.
8. NATO applicant countries; see RFE/RL, "Bulgarian Parliament Starts to Vote on Classified Information Protection Law," Newline, Prague, April 18, 2002. – http://cio.gov/Documents/computer_security.html.
9. The Canadian government published the revised agreement, "Agreement between the Parties to the North Atlantic Treaty for the Security of Information," as Canada Treaty Series, document 1998/56. – <http://csrc.ncsl.nist.gov/publications/nistpubs/index.html>.
10. NATO Office of Security, Letter from Mr. Wayne Rychak, Director, to Mr. Jacob Visscher, General Secretariat of the Council of the European Union (Brussels: NATO Office of Security, February 6,2002). – http://cio.gov/Documents/computer_security_act_Jan_1998.html.
11. NATO, Security within the North Atlantic Treaty Organization (Brussels: NATO Archives, reissued July 31, 1964), enc. "B," par. 1. – <http://www.c3i.osd.mil/org/cio/doc/gigia061600.pdf>.
12. Edition of C-M(55)15(Final) and will be referred to as NATO 1964. For the first edition of this document, see note 37 below. NATO 1964, enc. "C," sec. II. – <http://www.nato.int>.
13. Security Committee, A Short Guide to the Handling of Classified Information (Brussels: NATO Archives, August 22, 1958), AC/35-WP/I4, p. 4. – <http://www.dtic.mil/whs/directives/corresd520028p.pdf>
14. NATO 1964, enc. "C," sec. V; see also NATO, Agreement Between the Parties to the North Atlantic Treaty for the Security of Information (with Annexes): In Force August 16, 1998, Canada Treaty Series 1998/56, art. 1. – <http://www.c3i.osd.mil/org/cio/doc/gigia061600.pdf>.
15. NATO' s Security Policy and the Entrenchment of State Secrecy.» Forthcoming in Cornell International Law Journal 26, no. 2 (May 2003). – http://cio.gov/Documents/computer_security_act_Jan_1998.html.
16. C-M(55)25; NATO, Note by the Secretary-General and Vice-Chairman of the Council on Security Procedures for the Protection of NATO Classified Information (Brussels: NATO Archives, March 8, 1955). – http://cio.gov/Documents/computer_security_act_Jan_1998.html.
17. Security Committee, Summary Record of NATO Security Committee Meeting, January 24–28, 1955 (Brussels: NATO Archives, February 8, 1955), AC/35-R/11, p. 1. – http://www.fas.org/irp/doddir/doe/o5635_4.htm.

18. North Atlantic Council, Summary Record of the Meeting of the Council on March 2, 1955 (Brussels: NATO Archives, March 2, 1955), C-R(55)8. – <http://rr.sans.org/policy/sensitive.php>.
19. NATO, Summary Record of the Meeting of the NATO Security Committee (Brussels: NATO Archives, October 17–18, 1957). – <http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf>.
20. Information and Documents (Brussels: NATO Archives, January 11, 1958), AC/35-D/226. – <http://csrc.ncsl.nist.gov/publications/nistpubs.html>.

The withheld document is NATO AC/35-R/23, the summary record of the meeting of the NATO Security Committee held on July 16–17, 1958. – <http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf>.

Адреса розміщення робочої програми навчальної дисципліни

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

7. Дані про перегляд робочої програми навчальної дисципліни¹

№ п/п	Дата, номер протоколу засідання кафедри (спільного засідання кафедр)	Рішення за результатами перегляду	Підпис керівника кафедри

¹ Перегляд робочої програми навчальної дисципліни відбувається щорічно, з урахуванням результатів моніторингу та періодичного перегляду освітньої програми і, зокрема, отриманих від здобувачів вищої освіти та інших стейкхолдерів побажань та зауважень.

*29/3/4-503/4
18.10.2024*