МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
Харківський національний університет внутрішніх справ
Факультет № 4
Кафедра протидії кіберзлочинності

ЗАТВЕРДЖЕНО
На спільному засідання кафедри протидії кіберзлочинності факультету №4 та кафедри кібербезпеки та DATA-технологій факультету №6
Протокол № 2 від 22.06.2023 р.
Завідувач кафедри
Олександр МАНЖАЙ
_____

Лучик Світлана Дмитрівна

УПРАВЛІННЯ ТА ОРГАНІЗАЦІЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ (ОК.19)

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Кафедра	Протидії кіберзлочинності (https://univd.edu.ua/uk/dir/1740/kafedra-protydii-kiberzlochynnosti)
Контактний телефон	+38 057 7398085 (роб.)
E-mail	moj@univd.edu.ua
Офіційна назва освітньої програми	Кібербезпека та захист інформації (безпека інформаційних та комунікаційних систем) Cybersecurity and information protection (security of information and communication systems)
Рівень вищої освіти	Перший (бакалаврський) (НРК України – 6 рівень та перший цикл вищої освіти Рамки кваліфікацій Європейського простору вищої освіти)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека

Спеціалізація	Безпека інформаційних та комунікаційних систем
Статус дисципліни	Нормативна компонента освітньо-наукової програми, вивчається в 7-8 семестрі, на IV курсі навчання
Мова викладання	Українська
Обсяг дисципліни в кредитах ECTS/годинах	6 кредитів ECTS (загальний обсяг - 180 год.)
	- аудиторна робота: 90/18год., з них:
	лекції: 36/8 год.
	лабораторні заняття:
	практичні заняття: 46/10 год.
	семінарські заняття:
	самостійна робота: 90/162 год.
Час і місце проведення навчальної дисципліни	Аудиторія та час проведення заняття згідно розкладу
Консультації з навчальної дисципліни	Аудиторні консультації: аудиторія згідно графіку консультацій. Он-лайн-консультації: письмово в системі дистанційного навчання Moodle або електронною поштою викладача
Мета вивчення дисципліни	Метою викладання навчальної дисципліни «Управління та організація систем захисту інформації» є навчити здобувачів вищої освіти створювати і забезпечувати функціонування комплексної системи захисту інформації.
Завдання вивчення дисципліни	закладення знань та умінь із організації захисту інформації на об’єктах інформаційної діяльності як в підрозділах МВС України, так і в інших установах; формування навичок аналізу зарубіжних систем забезпечення інформаційної безпеки з метою впровадження найкращих практик захисту інформації.
Форми та види проведення навчальних занять	Форма навчання – денна, заочна. Види навчальних занять: лекції, практичні, самостійна робота.
Самостійна робота	Опрацювання рекомендованої літератури, поширене вивчення теоретичних питань лекційних занять за кожною темою, та опрацювання завдань з метою підготовки до практичних занять.
Необхідне обладнання	Комп’ютерний клас, мультимедійне обладнання (ноутбук та проектор), комп’ютерне забезпечення

	з виходом у мережу Інтернет.
Індивідуальні завдання	Наукові доповіді, індивідуальні завдання до лабораторних занять.
Контроль	***Методи контролю:*** - усний та письмовий; - тестовий. ***Форми контролю:*** - поточний; - підсумковий. Форми поточного контролю: захист індивідуальних завдань на лабораторних заняттях, тестування, перевірка аудиторних контрольних робіт, перевірка виконання самостійних робіт. Критерії оцінки поточного контролю викладач повідомляє на першому занятті та перед кожними оцінюванням. Форми підсумкового контролю: залік
Інтегральна компетентність, загальні компетентності, спеціальні (фахові) компетентності	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційних технологій (кібербезпека), що передбачає ідентифікацію та використання інформації для прийняття рішень ЗК 2. Здатність застосовувати знання на практиці. ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ФК 1. Здатність застосовувати нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. ФК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. ФК 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). ФК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. ФК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

	ФК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки

ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ЗА ТЕМАМИ

ТЕМА № 1. Основні положення щодо організації системи захисту інформації.

1. Умови безпеки інформації. Державна політика і система ТЗІ в Україні.
2. Нормативно-правова база України у сфері ТЗІ. Система захисту інформації у контексті системного мислення та системного підходу.

ТЕМА № 2. Визначення інформаційних ресурсів, що підлягають захисту.

1. Державна таємниця і конфіденційна інформація, що є власністю держави. Недержавна конфіденційна і відкрита інформація, що потребує захисту.
2. Дослідження структури і умов функціонування інформаційної системи організації. Модель системи об'єктів захисту.

ТЕМА № 3. Виявлення повної множини загроз безпеки інформаційним ресурсам, які підлягають захисту.

1. Класифікація загроз інформації. Технічні канали витоку інформації та НСД в комп'ютерних системах.
2. Окрема модель загроз. Джерела загроз і окрема модель порушника.

ТЕМА № 4. Проведення оцінки уразливості і ризиків для інформаційних ресурсів, що підлягають захисту, при виявленій множині загроз.

1. Оцінка вразливості інформаційних ресурсів.
2. Оцінка ризиків для інформаційних ресурсів.

ТЕМА № 5. Методи та засоби захисту інформації.

1. Методи і засоби захисту інформації від витоку по технічних каналах.
2. Основні положення "Критеріїв оцінки захищеності інформації в комп'ютерних системах від НСД".

ТЕМА № 6. Захист інформації в комп'ютерних системах від несанкціонованого доступу.

1. Основні положення "Загальних критеріїв".
2. Базова технічна модель IT-безпеки відповідно до NIST Special Publication 800-33.

ТЕМА № 7. Політика інформаційної безпеки.

1. Загальні положення щодо політики безпеки.
2. Зміст основних документів політики безпеки.

ТЕМА № 8. Розробка проекту системи захисту інформації.

1. Модель простору заходів і засобів захисту.
2. Критерій і особливості проектування оптимальної системи захисту інформації. Технічне завдання на розробку СЗІ і План захисту інформації.

ТЕМА № 9. Впровадження, визначення якості і управління системою захисту інформації. 1. Реалізація проекту (плану) захисту інформації. 2. Визначення якості реалізованої системи захисту. Контроль функціонування і управління системою захисту.	
ТЕМА № 10. Нормативно-правова база США щодо забезпечення інформаційної безпеки. 1. Поняття кіберпростору. Огляд основних законів щодо інформаційної безпеки кіберпростору. 2. Federal Information Security Management Act of 2002, FISMA. Класифікація нормативних документів з інформаційної безпеки.	
ТЕМА № 11. Структура забезпечення інформаційної безпеки (Information Security Governance). 1. Загальні вимоги забезпечення інформаційної безпеки. Складові забезпечення інформаційної безпеки. 2. Проблеми та шляхи їх вирішення у забезпеченні інформаційної безпеки.	
Результати навчання	ПР 7 Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки ПР 8 Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки ПР 9 Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки ПР 12 Розробляти моделі загроз та порушників ПР 16 Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів ПР 33 Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків ПР 34 Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації ПР 35 Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної та\або кібербезпеки ПР 39 Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням

	результатів у відповідних документах. ПР 44 Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами. ПР 46 Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
Форми поточного та підсумкового контролю	Поточний контроль – 50 балів. Підсумковий контроль –екзамен – 50 балів.
Критерії оцінювання	Оцінювання навчальної дисципліни проводиться за результатами поточного та підсумкового контролю: - поточний контроль - 50 балів; - підсумковий контроль - 50 балів. Оцінка за поточний контроль складається з оцінювання аудиторної та самостійної роботи здобувача вищої освіти. Оцінка за аудиторну роботу визначається як середнє арифметичне балів, які ним отримані на заняттях (здобувач має отримати не менш 5 позитивних оцінок) з коефіцієнтом 5. Оцінка за самостійну роботу визначається як середнє арифметичне балів, які отримані здобувачем за: наукові доповіді, індивідуальні завдання до лабораторних занять (здобувач має підготувати не менш 2 проектів) з коефіцієнтом 5. Підсумкові бали з навчальної дисципліни визначаються як сума балів, які отримані здобувачем протягом семестру, та балів, які набрані на підсумковому контролі (екзамені).

ШКАЛА ОЦІНЮВАННЯ: НАЦІОНАЛЬНА ТА ECTS			
Оцінка в балах	**Оцінка за національною шкалою**	**Оцінка за шкалою ECTS**	
		Оцінка	**Пояснення**
97-100 **94-96** **90-93**	Відмінно (“зараховано”)	A	**„Відмінно”** – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом сформовані, всі навчальні завдання, які передбачені програмою навчання виконані в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.

85-89	Добре (“зараховано”)	B	**„Дуже добре”** – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані, якість виконання більшості з них оцінено числом балів, близьким до максимального, робота з двома – трьома незначними помилками.
80-84			
75-79		C	**„Добре”** – теоретичний зміст курсу освоєний цілком, практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані, якість виконання жодного з них не оцінено мінімальним числом балів, деякі види завдань виконані з помилками, робота з декількома незначними помилками, або з однією – двома значними помилками.
70-74	Задовільно (“зараховано”)	D	**„Задовільно”** – теоретичний зміст курсу освоєний не повністю, але прогалинине носять істотного характеру, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, більшість передбачених програмою навчання навчальних завдань виконано, деякі з виконаних завдань, містять помилки, робота з трьома значними помилками.
65-69			
60-64		E	**„Достатньо”** – теоретичний зміст курсу освоєний частково, деякі практичні навички роботи не сформовані, частина передбачених програмою навчання навчальних завдань не виконані, або якість виконання деяких з них оцінено числом балів, близьким до мінімального,робота, що задовольняє мінімуму критеріїв оцінки.
40-59	Незадовільно („не зарахована”)	FX	**„Умовно незадовільно”** – теоретичний зміст курсу освоєний частково, необхідні практичні навички роботи не сформовані, більшість передбачених програм навчання, навчальних завдань не виконано, або якість їхнього виконання оцінено числом балів, близьким до мінімального; при додатковій самостійній роботі над матеріалом курсу можливе підвищення якості виконання навчальних завдань (з можливістю повторного складання), робота, що потребує доробки
21-40			
1-20		F	**„Безумовно незадовільно”** – теоретичний зміст курсу не освоєно, необхідні практичні навички роботи не сформовані, всі виконані навчальні

			завдання містять грубі помилки, додаткова самостійна робота над матеріалом курсу не приведе до значимого підвищення якості виконання навчальних завдань, робота, що потребує повної переробки
Орієнтовний перелік питань до заліку (екзамену)			***Теоретичні питання до заліку (7 семестр)*** 1. Що розуміється під терміном "інформація"? 2. Наведіть властивості інформації? 3. На що направлені загрози конфіденційності? 4. На що направлені загрози цілісності? 5. На що направлені загрози доступності? 6. Що розуміється під терміном "комунікабельні носії інформації"? 7. Що розуміється під терміном "режимна адекватність"? 8. Які є види інформації за режимом доступу? 9. Яка суть так званої парадигми захисту інформації? 10. Яким чином парадигма захисту інформації враховує основні інформаційні загрози? 11. Якими чинниками обумовлюється розвиток ТЗІ в Україні? 12. Які є основні загрози безпеці інформації в Україні? 13. Що є системою ТЗІ? 14. На яких принципах реалізується державна політика у сфері ТЗІ? 15. Хто виступає суб'єктами системи ТЗІ України? 16. Місія Держспецзв’язку в контексті забезпечення інформаційної безпеки. 17. Що складає правову основу технічного захисту інформації в Україні? 18. Як можна розділити нормативно-правову і методичну базу в сфері ТЗІ з урахуванням сфери застосування? 19. Що таке "інформаційна система"? 20. Що таке система, і якими є її властивості? 21. У чому полягають ключові характеристики системного мислення та системного підходу? 22. Якою є ієрархія за рівнем узагальнення і складності об’єктів узагальненої інформаційно-телекомунікаційної системи? 23. Як можна представити ієрархію за рівнем узагальнення і складності? 24. Як можна застосувати ключові характеристики системного мислення та системного підходу до моделі мережі взаємин CITS-ISCS? 25. Якими є основні кроки у визначенні інформаційних ресурсів, які підлягають захисту?

	26. Що є об'єктом обов'язкового захисту інженерно-технічними заходами? 27. Які основні поняття державної таємниці і конфіденційної інформації, що є власністю держави? 28. Що можна віднести до недержавної конфіденційної і відкритої інформації, яка потребує захисту, і як це зробити? 29. З яких кроків складається перший етап побудови СЗІ? 30. Який можливий порядок проведення експертизи з метою визначення Переліку конфіденційних відомостей організації? 31. На яких носіях може існувати інформація, що потребує захисту? 32. Які задачі вирішуються при обстеженні інформаційної системи організації? 33. Яке значення мають терміни: виділений об'єкт, контрольована зона, категоріювання об'єкту, основні технічні засоби, допоміжні технічні засоби і системи? 34. Що може відноситися до основних технічних засобів і систем? 35. Що може відноситися до допоміжних технічних засобів і систем? 36. Які вимоги до опису компонентів автоматизованої системи і технології обробки інформації? 37. Як можна представити модель системи інформаційних об'єктів захисту? 38. Як визначаються вагові коефіцієнти в моделі системи інформаційних об'єктів захисту? 39. Які документи необхідно мати після проведення робіт відповідно до першого етапу побудови системи захисту інформації? 40. Як можна класифікувати загрози інформації? 41. Що є технічними каналами витоку інформації? 42. Як можна класифікувати технічні канали витоку інформації? 43. Як за допомогою схеми можна представити можливі канали витоку інформації у типовому одноповерховому приміщенні? 44. Як за допомогою схеми можна представити несанкціонований доступ до інформації у типовому одноповерховому приміщенні? 45. Як можна описати і представити загрози в окремій моделі загроз? 46. Які розділи доцільно включити в окрему модель загроз об'єкту інформаційної діяльності? 47. Наведіть класифікацію джерел загроз інформаційної

	безпеки? 48. Наведіть перелік джерел загроз інформаційної безпеки? 49. Яким методом можна провести ранжирування джерел загроз інформаційної безпеки? 50. За природою походження якими можуть бути джерела загроз? 51. Наведіть основні групи джерел загроз. 52. Наведіть основні типи реалізації загроз. 53. Наведіть методи ранжирування джерел загроз. 54. За допомогою яких способів можуть реалізовуватися загрози? 55. Кваліфікація антропогенних джерел. 56. Як визначається ступінь неусувності наслідків прояву загрози (фатальність)? 57. Наведіть відмінності у поняттях «порушник» та «зловмисник». 58. Модель порушника: поняття, характеристика. 59. Яка класифікація використовується при створенні окремої моделі порушника? 60. Які документи необхідно мати після проведення робіт відповідно до другого етапу побудови системи захисту інформації, і який їх зміст? 61. Наведіть визначення терміну «уразливість». 62. Якими недоліками обумовлюються вразливості, що є властивостями ОІД? 63. Наведіть класифікацію уразливостей інформаційних ресурсів? 64. Наведіть перелік уразливостей інформаційних ресурсів? 65. Що належить до об'єктивних уразливостей? 66. Що належить до суб'єктивних уразливостей? 67. Що належить до випадкових уразливостей? 68. Що належить до психогенних уразливостей? 69. Яким методом можна провести ранжирування вразливостей інформаційних ресурсів? 70. Як можна представити і показати модель дії загроз на множину об'єктів захисту і існуючої системи захисту інформації? 71. Як визначаються вагові коефіцієнти в моделі дії загроз на множину об'єктів захисту і існуючої системи захисту інформації? 72. Яким чином визначаються інформаційні ризики, і здійснюється управління ними? 73. Що розуміють під управлінням ризиками? 74. Наведіть методи визначення ризиків для ОІД.

	75. Які документи необхідно мати після проведення робіт відповідно до третього етапу побудови системи захисту інформації, і який їх зміст? 76. Якими можуть бути організаційні заходи захисту інформації від витоку технічними каналами? 77. Якими можуть бути первинні технічні заходи захисту інформації від витоку технічними каналами? 78. На яких принципах базуються основні технічні заходи захисту інформації від витоку технічними каналами, і яка їх суть? 79. Що відноситься до спеціальних засобів ТЗІ? 80. Що передбачають основні технічні заходи? 81. Яка суть заходів щодо блокування ТКВІ з використанням пасивних засобів? 82. Яка суть заходів щодо блокування ТКВІ з використанням активних засобів? 83. Яка суть заходів щодо виявлення портативних електронних пристроїв перехоплення інформації? 84. Якими є основні поняття теорії захисту інформації в комп'ютерних системах? 85. Які існують підходи в представленні моделі довільної комп'ютерної системи, і в чому їх суть? 86. На рішення яких проблем спрямовані стандарти інформаційної безпеки? 87. Які стандарти інформаційної безпеки найбільш відомі? 88. Які поняття об'єкту інформаційного обміну використовуються в "Критеріях оцінки захищеності інформації в комп'ютерних системах від НСД"? 89. З чого складається загальна оцінка рівня безпеки системи? 90. Які послуги передбачають критерії конфіденційності в "Критеріях оцінки захищеності інформації в комп'ютерних системах від НСД", і в чому їх суть? 91. Які послуги передбачають критерії цілісності в "Критеріях оцінки захищеності інформації в комп'ютерних системах від НСД", і в чому їх суть? 92. Які послуги передбачають критерії доступності в "Критеріях оцінки захищеності інформації в комп'ютерних системах від НСД", і в чому їх суть? 93. Які послуги передбачають критерії спостереженості в "Критеріях оцінки захищеності інформації в комп'ютерних системах від НСД", і в чому їх суть? 94. Які розділи включають критерії гарантій "Критерії оцінки захищеності інформації в комп'ютерних системах від НСД"?

	95. Що є стандартними функціональними профілями захищеності, і як вони описуються? 96. Які ключові поняття використовуються в "Загальних критеріях"? 97. Як можна представити схему оцінки безпеки ІТ-продукту на основі "Загальних критеріїв"? 98. Якою є структура і розділи Профілю захисту "Загальних критеріїв"? 99. Якою є структура і розділи Проекту захисту "Загальних критеріїв"? 100. Якою є ієрархія і ознаки поділу функціональних вимог "Загальних критеріїв"? 101. Якою є таксономія класів функціональних вимог "Загальних критеріїв", і в чому їх суть? 102. Якою є таксономія сімейств функціональних вимог для всіх класів "Загальних критеріїв"? 103. Що включає розділ "Загальних критеріїв", який описує вимоги адекватності? 104. Якою є таксономія вимог адекватності "Загальних критеріїв", і в чому їх суть? 105. Як характеризуються стандартні рівні адекватності "Загальних критеріїв"? 106. Якою є головна мета і завдання ІТ-безпеки відповідно до NIST Special Publication 800-33? 107. Як залежать одна від одної задачі ІТ-безпеки? 108. Яким чином можна представити модель взаємодії послуг безпеки в ІТ-системах? 109. У чому полягає суть послуг безпеки в ІТ-системах? 110. Які потрібні послуги для вирішення задач доступності та цілісності в моделі взаємодії послуг безпеки в ІТ-системах? 111. Які потрібні послуги для вирішення задач спостереженості та гарантій в моделі взаємодії послуг безпеки в ІТ-системах? 112. Як можна представити взаємну залежність розподілених сервісів безпеки відповідно до NIST Special Publication 800-33? 113. За рахунок чого можуть бути збільшені гарантії системи відповідно до NIST Special Publication 800-33? 114. У чому полягає суть концепції доменів безпеки для ІТ-безпеки мереж? 115. Яким є алгоритм зменшення інформаційних ризиків при наявності навмисних і ненавмисних джерел загроз? 116. Яку роль в СЗІ виконує політика безпеки? 117. Яка модель організацій з позиції їх зрілості в сфері інформаційної безпеки запропонована Carnegie Mellon

	University? 118. У вигляді яких документів доцільно оформляти політику безпеки організації? 119. Які цілі політики безпеки організації? 120. Які завдання політики безпеки організації? 121. Наведіть основні обов'язки керівників організації в сфері інформаційної безпеки. 122. Наведіть основні обов'язки працівників відділу (підрозділу) інформаційної безпеки організації в сфері інформаційної безпеки. 123. Які обов'язки адміністраторів безпеки, адміністраторів КС, працівників організації в сфері інформаційної безпеки? 124. Які можуть бути вимоги політики безпеки організації щодо забезпечення фізичної безпеки комп'ютерної системи? 125. Які можуть бути загальні вимоги політики безпеки організації щодо управління і використання комп'ютерної системи? 126. Які можуть бути правила безпеки при використанні зовнішніх ресурсів (Internet)? 127. Які можуть бути правила безпеки при використанні електронної пошти? 128. Які можуть бути вимоги політики безпеки організації щодо організації антивірусного захисту комп'ютерної системи? 129. Які можуть бути вимоги політики безпеки організації щодо управління і експлуатації криптографічних систем в комп'ютерній системі? 130. Які можуть бути правила впровадження програмного забезпечення в контексті безпеки? 131. Що є зобов'язанням виконання Політики безпеки організації? 132. Як можна визначити порядок впровадження і контролю виконання політики безпеки? 133. Яким може бути порядок перегляду політики безпеки? 134. У вигляді якої структури можна представити простір СЗІ? 135. Наведіть основні елементи структури простору СЗІ. 136. Що відноситься до заходів і засобів, що забезпечують основну діяльність організації? 137. Що належить до основних заходів і засобів організації? 138. Яке завдання розв'язується при оптимізації СЗІ? 139. За якими критеріями розв'язується завдання оптимізації СЗІ? 140. Наведіть особливості задач, що вирішуються при проектуванні СЗІ? 141. Наведіть послідовність задач, що вирішуються при

	проектуванні СЗІ? 142. Які розділи передбачає Технічне завдання на розробку СЗІ? 143. Які розділи передбачає План захисту інформації? 144. Що можна передбачити як організаційні заходи щодо реалізації проекту (плану) захисту інформації? 145. Які розділи має містити календарний план захисту інформації? 146. Що належить до контрольно-правових заходів щодо реалізації проекту (плану) захисту інформації? 147. Що належить до профілактичних заходів щодо реалізації проекту (плану) захисту інформації? 148. Що належить до інженерно-технічних заходів щодо реалізації проекту (плану) захисту інформації? 149. Відповідно до вимог затвердженого ТЗ на створення КТЗІ розроблюється пояснювальна записка з ТЗІ. Що у ній зазначається? 150. Наведіть вимоги до оформлення акту приймання робіт з ТЗІ. 151. Що передбачає випробування КТЗІ? 152. Що вказують у "Висновках за результатами випробувань комплексу ТЗІ"? 153. Який зміст етапу "визначення якості реалізованої системи захисту"? 154. Які є види державної експертизи? 155. Який порядок організації державної експертизи? 156. Який порядок проведення державної експертизи? 157. Які документи необхідно мати у результаті проведення державної експертизи СЗІ? 158. Які є види атестації? 159. Який порядок організації атестації? 160. Який порядок проведення атестації? 161. Які документи необхідно мати у результаті проведення атестації СЗІ? 162. Які документи необхідно мати після проведення робіт відповідно до шостого етапу побудови системи захисту інформації? 163. Який зміст документів, що необхідно мати після проведення робіт відповідно до шостого етапу побудови системи захисту інформації? 164. У чому суть контрольно-інспекційної роботи з питань ТЗІ щодо суб'єктів системи ТЗІ? 165. Які є види перевірок СЗІ? 166. На які категорії розділяють порушення встановлених норм і вимог ТЗІ, виявлених під час проведення перевірок?

	167. Які документи складаються за результатами перевірок стану ТЗІ посадовими особами Держспецзв'язку? 168. Які документи необхідно мати після проведення робіт відповідно до сьомого етапу побудови системи захисту інформації? 169. Який зміст документів, що необхідно мати після проведення робіт відповідно до сьомого етапу побудови системи захисту інформації? 170. Якими основними ознаками характеризується кіберпростір? 171. Наведіть визначення терміну «кіберпростір». 172. Що таке юрисдикція? 173. Яким є правовий режим Інтернет? 174. Який закон США вперше містив визначення терміну «електронний підпис»? 175. Наведіть основні вимоги Закону США про конфіденційність електронних повідомлень (Electronic Communications Privacy Act of 1986, ECPA). 176. Наведіть основні вимоги Закону США про звітність і перенесення даних про страхування здоров'я громадян (Health Insurance Portability and Accountability Act of 1996, HIPAA). 177. Наведіть основні вимоги Закону Клінжера-Коена (Clinger-Cohen Act of 1996, CCA), званий також Законом про реформу управління інформаційними технологіями (Information Technology Management Reform Act). 178. Наведіть основні вимоги Федерального закону США «Government Paperwork Elimination Act of 1998». 179. Наведіть основні вимоги Правил стандартного діловодства (Standard Transaction Rule, STR). 180. Який закон США вперше дав офіційне тлумаченням терміну «інформаційна технологія»? 181. Наведіть основні вимоги стандарту «Standards for Privacy and Individually Identifiable Information». 182. Наведіть основні вимоги закону Гремма-Ліча-Блілі (Gramm-Leach-Bliley Act of 1999, GLBA) або Акту про модернізацію фінансових послуг (Financial Services Modernization). 183. Наведіть три основні вимоги щодо захисту персональних відомостей про громадян, що були сформульовані у Законі GLBA (Gramm-Leach-Bliley Act of 1999). 184. Наведіть основні вимоги Акту про контамінації комп'ютерів (Computer Contaminant Act of 2000). 185. Наведіть основні вимоги закону США Uniting and Strengthening America by Providing Appropriate Tools Required to

	Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act of 2001). 186. Наведіть основні вимоги закону США про реформування звітності компаній і захисту інвесторів (Public Company Accounting Reform and Investor Protection Act of 2002). 187. Наведіть основні вимоги закону США про управління федеральної інформаційною безпекою (Federal Information Security Management Act of 2002, FISMA). 188. Наведіть основні вимоги документу «Захист кіберпростору Америки - Національний план із захисту інформаційних систем. Версія 1.0». (Defending America's Cyberspace - National Plan for Information System Protection. Version 1.0). 189. Наведіть основні вимоги «Національної стратегії щодо захисту кіберпростору» (National Strategy to Secure Cyberspace of 2003). 190. Наведіть п'ять національних пріоритетів, визначених «Національною стратегією щодо захисту кіберпростору» (National Strategy to Secure Cyberspace of 2003). 191. Наведіть основні стратегічні цілі Національної стратегії США щодо захисту кіберпростору. 192. Який закон США відображає намір уряду США захистити власні комп'ютерні мережі? 193. Яка організація безпосередньо розробляє різні типи документів з інформаційної безпеки США? 194. Які типи документів з інформаційної безпеки публікує Computer Security Division? 195. Які інституції визначають вимоги з ІБ та впливають на забезпечення інформаційної безпеки федеральних організацій США? 196. Яким чином інституції США визначають вимоги з ІБ та впливають на забезпечення інформаційної безпеки федеральних організацій? 197. Якими є основні види діяльності щодо інтегрування заходів інформаційні безпеки в загальну структуру організації США? 198. У чому суть стратегічного планування інформаційної безпеки у федеральній агенції США? 199. Якими можуть бути структури забезпечення ІБ у федеральній організації США? 200. Які типові посади (ролі), що мають відношення до ІБ, характерні для більшості організацій? 201. Хто такий Федеральний Корпоративний Архітектор? 202. Яке відношення Федеральний Корпоративний Архітектор має до ІБ організацій?

	203. У чому полягає політика інформаційної безпеки установи США? 204. Наведіть основні вимоги нормативного документу США "National Institute of Standards and Technology Special Publication 800-100, Information Security Handbook: A Guide for Managers. Recommendations of the National Institute of Standards and Technology, October 2006". 205. Наведіть основні компетенції Office of Management and Budget (OMB). 206. Наведіть основні компетенції Government Accountability Office (GAO). 207. Наведіть основні вимоги закону США The Government Performance and Results Act (GPRA) of 1993. 208. Наведіть основні вимоги The Paperwork Reduction Act (PRA) of 1995. 209. Наведіть основні вимоги The Federal Financial Management Improvement Act (FFMIA) of 1996. 210. Наведіть основні вимоги The Federal Managers Financial Integrity Act (FMFIA) of 1982. 211. Наведіть основні вимоги The Clinger-Cohen Act of 1996. 212. Наведіть основні вимоги The E-Government Act of 2002 (Public Law 107-347). 213. Наведіть основні повноваження у сфері інформаційної безпеки CIO департаменту (chief information officer). 214. Наведіть основні повноваження у сфері інформаційної безпеки SAISO (senior agency information security officer). 215. Наведіть основні повноваження у сфері інформаційної безпеки Chief Enterprise Architect (головного корпоративного архітектора). 216. Наведіть основні повноваження у сфері інформаційної безпеки організації Inspector General (IG) (генерального інспектора). 217. Наведіть основні повноваження у сфері інформаційної безпеки організації Chief Financial Officer (головного фінансового офіцера). 218. Наведіть основні повноваження у сфері інформаційної безпеки Chief Privacy Officer (головного офіцера з питань конфіденційності). 219. Наведіть основні повноваження у сфері інформаційної безпеки Physical Security Officer (офіцера фізичної безпеки). 220. Наведіть основні повноваження у сфері інформаційної безпеки Personnel Security Officer (офіцера персональної безпеки). 221. Які фактори впливають на те, що з часом політики та процедури ІБ можуть стати неадекватними?

	Теоретичні питання до екзамену (8 семестр) 1.
Рекомендована література **Основна**	1. Бабак В.П., Ключников А.А. Теоретичні основи захисту інформації: підручник. НАН України, Ін-т проблем безпеки АЕС. Чорнобиль (Київ.обл.): Ін-т проблем безпеки АЕС, 2012. 776 с. 2. Гулак Г.М Методологія захисту інформації. Аспекти кібербезпеки: підручник. К.: Видавництво НА СБ України, 2020. 256 с. 3. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. К., 2013. 435 с., іл.160. 4. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. посібник. Дніпро: Дніпроп. держ. Ун-т внутріш. справ, 2020. 144 с. 5. Гур'єв В.І., Мехед Д.Б., Ткач Ю.М., Фірсова І.В. Ніжин: ФОП Лук'яненко В.В. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ ТПК «Орхідея», 2018. 166 с. 6. Захарченко М.В., Кононович В.Г., Кільдішев В.Й., Голев Д.В. Інформаційна безпека інформаційно-комунікаційних систем. Лабораторний практикум. Частина 1 – Комплекси засобів захисту інформації від НСД: навч. посіб. / // За ред. ак. МАІ М.В. Захарченка. Одеса: ОНАЗ ім. О.С. Попова, 2011. – 168 с. 7. Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник. К.: ІСЗЗІ НТУУ. «КПІ», 2016. 104 с. 8. Інформаційна безпека держави. Конспект лекцій для здобувачів вищої освіти освітнього ступеню «бакалавр» спеціальності 262 – «Правоохоронна діяльність». Укл.: Ю.М. Ткач, С.М. Семендяй. Чернігів: НУ «Чернігівська політехніка», 2022. 133 с. 9. Кравець П. І., Шимкович В.М., Бердник Ю.М. Інформаційно-керуючі системи. Локальні інформаційно-керуючі системи. Лабораторний практикум. Навчальний посібник. К: КПІ ім. Ігоря Сікорського, 2022. 142 с. 10. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с. 11. ДСТУ ISO/IEC 19989-1:2023 (ISO/IEC 19989-1:2020, IDT) Інформаційна безпека. Критерії та методологія оцінювання безпеки біометричних систем. Частина 1. Структура

	12. ДСТУ ISO/IEC 19989-2:2023 (ISO/IEC 19989-2:2020, IDT) Інформаційна безпека. Критерії та методологія оцінювання безпеки біометричних систем. Частина 2. Ефективність біометричного розпізнавання 13. ДСТУ ISO/IEC 24745:2023 (ISO/IEC 24745:2022, IDT) Інформаційні технології. Кібербезпека та захист конфіденційності. Захист біометричної інформаці 14. ДСТУ ISO/IEC 15408-1:2023 ISO/IEC 15408-1:2022, IDT) Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 1. Вступ та загальна модель 15. ДСТУ ISO/IEC 15408-2:2023 (ISO/IEC 15408-2:2022, IDT) Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 2. Функційні компоненти безпеки 16. ДСТУ ISO/IEC 15408-3:2023 (ISO/IEC 15408-3:2022, IDT) Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 3. Компоненти убезпечення. 17. ДСТУ ISO/IEC 15408-4:2023 (ISO/IEC 15408-4:2022, IDT) Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 4. Структура для визначення методів оцінювання та діяльності 18. ДСТУ ISO/IEC 15408-5:2023 (ISO/IEC 15408-5:2022, IDT) Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 5. Попередньо визначені пакети вимог до безпеки 19. ДСТУ ISO/IEC 18045:2023 (ISO/IEC 18045:2022, IDT) Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Методологія оцінювання безпеки ІТ 20. ДСТУ ISO/IEC 30107-1:2023 (ISO/IEC 30107-1:2016, IDT) Інформаційні технології. Виявлення атак на біометричне подання. Частина 1. Структура 21. ДСТУ ISO/IEC 30107-2:2023 (ISO/IEC 30107-2:2017, IDT) Інформаційні технології. Виявлення атак на біометричне подання. Частина 2. Формати даних. 22. ДСТУ ISO/IEC 30107-3:2023 (ISO/IEC 30107-3:2017, IDT) Інформаційні технології. Виявлення атак на біометричне подання. Частина 3. Тестування та звітування 23. ДСТУ ISO/IEC 30107-4:2023 (ISO/IEC 30107-4:2020, IDT) Інформаційні технології. Виявлення атак на біометричне подання. Частина 4. Профіль для тестування мобільних пристроїв. 24. ДСТУ ISO/IEC 29146:2023 (ISO/IEC 29146:2016, IDT).

	Інформаційні технології. Методи безпеки. Структура керування доступом. 25. ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT). Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги. 26. ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки. 27. ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT) Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки. 28. ДСТУ ISO/IEC 27551:2023 (ISO/IEC 27551:2021, IDT). Інформаційна безпека, кібербезпека та захист конфіденційності. Вимоги до автентифікації непов'язаних об'єктів на основі атрибутів. 29. НД ТЗІ 1.1-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. 30. НД ТЗІ 1.1-002-99.Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу. 31. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. 32. НД ТЗІ 1.1-004-2003 Протидія технічним розвідкам. Терміни та визначення. 33. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. 34. НД ТЗІ 1.6-002-03. Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації. 35. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації. 36. НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці”, затверджене наказом Адміністрації Держспецзв'язку від 15.04.2013 № 215. 37. НД ТЗІ 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу ТЗІ. Основні положення. 38. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в

	автоматизованих системах класу “2”. 39. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. 40. НД ТЗІ 2.7-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт. 41. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. 42. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (Зі зміною № 1). 43. НД ТЗІ 3.7-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова). 44. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. 45. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Постанова КМ України від 29.03.2006 № 373. 46. Положення про технічний захист інформації в Україні. Указ Президента України від 27.09.1999 № 1229. 47. Про Державну службу спеціального зв’язку та захисту інформації України. Закон України від 23.02.2006 № 3475-IV. 48. Про державну таємницю. Закон України від 21.01.1994 № 3855-XII. 49. Про деякі питання захисту інформації, охорона якої забезпечується державою. Постанова КМ України від 13.03.2002 № 281. 50. Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах. Постанова КМ України від 16.02.1998 № 180. 51. Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах. Постанова КМ України від 16.11.2002 № 1772. 52. Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Постанова Кабінету Міністрів України від 16 травня 2023 р. № 497. Київ. URL:

	https://zakon.rada.gov.ua/laws/show/497-2023-%D0%BF#Text 53. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 05.07.1994 № 80/94-ВР. 54. Про захист персональних даних. Закон України від 01.06.2010 № 2297-VI. 55. Про інформацію. Закон України від 02.10.1992 № 2657-XII.
Допоміжна література	1. Federal Information Security Management Act of 2002 (FISMA): Закон Федерального Уряду США по управлінню інформаційною безпекою. 2. National Institute of Standards and Technology Special Publication 800-100, Information Security Handbook: A Guide for Managers. Recommendations of the National Institute of Standards and Technology, October 2006. 3. National Institute of Standards and Technology Special Publication 800-64, Security Considerations in the Information System Development Life Cycle, Rev. 2, October 2008. 4. National Institute of Standards and Technology Special Publication 800-50, Building an Information Technology Security Awareness and Training Program, October 2003. 5. NIST SP 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model. 6. National Institute of Standards and Technology Special Publication 800-65, Integrating Information Security into the Capital Planning and Investment Control Process, January 2005. 7. National Institute of Standards and Technology Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems, August 2002. 8. National Institute of Standards and Technology Special Publication 800-55, Security Metrics Guide for Information Technology Systems, Revision 1, July 2008. 9. National Institute of Standards and Technology Special Publication 800-18, Guide for Developing Security Plans for Federal Information Systems, February 2006. 10. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Contingency Planning for Information Technology Systems, June 2002. 11. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems, July 2002. 12. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-36, Guide to Selecting Information Technology Security Products, October 2003. 13. Standards and Technology (NIST) Special Publication (SP)

	800-61, Computer Security Incident Handling Guide, March 2008.
Інформаційні ресурси в Інтернеті	1. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=88291&cat_id=38828 2. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=300864&cat_id=38829 3. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/category?cat_id=38834 4. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=306436&cat_id=38835&ctime=1554728725967 5. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/category?cat_id=38836 6. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=317914&cat_id=317913