

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
Кафедра комп'ютерних технологій та інформаційної безпеки

Код за ОПІ
ОК10

ЗАТВЕРДЖУЮ



Проректор з науково-педагогічної
роботи, к.т.н., доцент

С.О. Слободян

_____ 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Program of the Discipline

МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
INFORMATION SECURITY MANAGEMENT

Рівень вищої освіти _____ другий (магістерський) _____
Тип дисципліни _____ обов'язкова _____
Мова викладання _____ українська _____

Миколаїв 2025 рік

Робоча програма навчальної дисципліни «Менеджмент інформаційної безпеки» є однією із складових комплексної підготовки фахівців галузі знань «Інформаційні технології», спеціальності «ІТ Кібербезпека та захист інформації», освітня програма «Системи технічного захисту інформації, автоматизація її обробки»
 «24» 04 2025 р. – 29 с.

Розробник: Сірівчук А.С., доцент кафедри Комп'ютерних технологій та інформаційної безпеки, канд. техн. наук

Проект робочої програми навчальної дисципліни «Менеджмент інформаційної безпеки» узгоджено з гарантом освітньої програми
 Гарант освітньої програми «Системи технічного захисту інформації, автоматизація її обробки»
 Передерій В.І., д. т. н.

Проект робочої програми навчальної дисципліни «Менеджмент інформаційної безпеки» розглянуто на засіданні кафедри КТІБ.
 Протокол від «24» 04 2025 р. № 12.
 Завідувач кафедри КТІБ, к.т.н., доцент С.М. Нужний

Проект робочої програми навчальної дисципліни «Менеджмент інформаційної безпеки» розглянуто методичною радою Навчально-наукового інституту автоматики та електротехніки.
 Протокол від «15» 05 2025 р. № 5.
 Заступник голови МР ННІАЕ, к.т.н., доц. С.М.Новогрецький

Проект робочої програми навчальної дисципліни «Менеджмент інформаційної безпеки» погоджено з навчальним відділом.
 Начальник навчального відділу, к.т.н., доцент А.В. Лабарткава

Робочу програму навчальної дисципліни «Менеджмент інформаційної безпеки» затверджено Навчально-методичною радою НУК ім. адм. Макарова.
 Протокол від «21» 05 2025 р. № 5.

Голова Навчально-методичної ради НУК ім. адм. Макарова,
 к.т.н., доцент С.О.Слободян

ЗМІСТ

Вступ.....	4
1. Опис навчальної дисципліни	5
2. Мета навчальної дисципліни	6
3. Передумови для вивчення навчальної дисципліни	7
4. Очікувані результати навчання	7
5. Програма навчальної дисципліни	9
6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування.....	13
7. Форми поточного та підсумкового контролю	15
8. Критерії оцінювання результатів навчання.....	17
9. Засоби навчання	19
10. Рекомендовані джерела інформації.....	20

ВСТУП

Анотація

Навчальна дисципліна «Менеджмент інформаційної безпеки» є дисципліною професійної підготовки магістрів за освітньою програмою «Системи технічного захисту інформації, автоматизація її обробки» галузі знань «F Інформаційні технології», спеціальності «F5 Кібербезпека та захист інформації». Дана дисципліна є обов'язковим компонентом освітньої програми, який забезпечує формування умінь використовувати різноманітні методи оцінювання ефективності систем захисту інформації на основі різних критеріїв для забезпечення необхідного рівня захищеності інформації в автоматизованих, інформаційних і комунікаційних системах. Отримані слухачами курсу теоретичні знання та практичні навички є базовим програмним результатом навчання та формують фахову компетентність.

Важливість засвоєння теоретичних знань і здобуття практичних навичок оцінювання ризиків та інших показників якості систем захисту інформації обумовлена необхідністю їх моніторингу, аудиту та адаптації до динамічних умов експлуатації автоматизованих, інформаційних і комунікаційних систем. Основна увага в процесі викладання дисципліни приділяється вивченню методів вирішення актуальних прикладних задач інформаційної безпеки.

Ключові слова: критерії оцінювання ефективності систем захисту інформації, ризики інформаційної безпеки, методики оцінювання ризиків, нормативно-правове забезпечення менеджменту інформаційної безпеки.

Abstract

The educational discipline "Information security management" is a discipline of professional training for masters under the educational program "Systems of technical protection of information, automation of its processing" of the field of knowledge "F Information technology", specialty "F5 Cybersecurity and Information Protection ". This discipline is a mandatory component of the educational program, which provides the formation of the ability to use various methods of evaluating the effectiveness of information protection systems based on various criteria to ensure the necessary level of information security in automated, information and communication systems. The theoretical knowledge and practical skills acquired by the students of the course are the basic program outcome of the study and form professional competence.

The importance of acquiring theoretical knowledge and acquiring practical skills of risk assessment and other quality indicators of information protection systems is due to the need for their monitoring, auditing and adaptation to dynamic operating conditions of automated, information and communication systems. The main attention in the process of teaching the discipline is given to the study of methods of solving actual applied problems of information security.

Keywords: criteria for evaluating the effectiveness of information protection systems, information security risks, risk assessment methods, regulatory and legal support for information security management

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів – 4	Галузь знань F Інформаційні технології Спеціальність: F5 Кібербезпека та захист інформації	Обов’язкова	
Модулів – 1	Освітня програма «Системи технічного захисту інформації, автоматизація її обробки»	Рік підготовки	
Змістових модулів – 2		1-й	1-й
		Семестр	
Загальна кількість годин – 90		2-ий	2-ий
Тижневих годин для денної форми навчання: Аудиторних – 2 Самостійної роботи: – 4.	Рівень вищої освіти: другий (магістерський)	Лекції, год	
		15 год.	4 год.
		Лабораторні роботи, год	
		15 год.	8 год.
		Практичні роботи, год	
		-	-
		Самостійна робота, год	
		60	78
		Вид контролю: Екзамен	
		Форма контролю: усна, письмова	

2. Мета навчальної дисципліни

Метою вивчення навчальної дисципліни «Менеджмент інформаційної безпеки» є оволодіння здобувачами вищої освіти теоретичними методами і практичними методиками побудови і налагодження ефективних систем захисту автоматизованих, інформаційних і комунікаційних систем.

Завданнями дисципліни є теоретична та практична підготовка студентів для вирішення конкретних фахових питань, зокрема: обґрунтування прийняття проектних та експертних рішень в галузі менеджменту інформаційної безпеки; здобуття практичних навичок застосування спеціалізованого нормативно-правового (для студентів, що мають форму допуску до складу нормативно-правової бази включені документи з обмеженим доступом) і програмного забезпечення для вирішення задач менеджменту інформаційної безпеки на різних об'єктах інформаційної діяльності для формування наступних компетентностей:

Загальні компетентності

- (ЗК-1) - Здатність застосовувати знання у практичних ситуаціях;
- (ЗК-2) - Здатність проводити дослідження на відповідному рівні.;
- (ЗК-4) - Здатність оцінювати та забезпечувати якість виконуваних робіт;
- (ЗК-7) - Здатність до адаптації та дії у новій ситуації;

Фахові компетентності:

– (КФ-1)(А1) - Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки;

– (КФ-2)(А9) - Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки;

– (КФ-4)(А4) - 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)(А2) - 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;

- (КФ9)(В) - 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;

- (КФ15)(А8) - Здатність адмініструвати системи, мережі та системи безпеки інформації;

- (КФ17)(Г2) - Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимог технічного та організаційного спрямування щодо системи технічного криптографічного захисту інформації.

3. Передумови для вивчення навчальної дисципліни

Передумов для вивчення навчальної дисципліни «Менеджмент інформаційної безпеки» немає.

4. Очікувані результати навчання

Основними (програмними) результатами навчання з дисципліни «Менеджмент інформаційної безпеки» є:

- (РН-5)(А2.34, А3.31, Г1.31, А1.У4, А3.У5, В3.У1, В4.У2) – Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення;

- (РН-7)(А3.35, А3.36, В1.33, Г1.36, Б2.У1, Г2.У3) – Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки;

- (РН-8)(А2.36, Г1.31, Г1.33, Г2.31, Д1.31, А1.У4, Г1.У2, Г2.У3, Г2.У4, Д1.У3, Д1.У4) – Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури;

- (РН-9)(А1.34, Б2.32, В1.31, В4.31, Д1.34, А1.У1, А2.У2, Б1.У1, Г1.У1, Г1.У3, Г1.У4, Д1.У4) – Аналізувати, розробляти і супроводжувати систему

управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки;

– (РН-10)(A1.35, A1.37, A2.31, B1.31, B1.31, Д1.32, Д2.31, A1.У1, A1.У4, B1.У1, B2.У1, B3.У1, B4.У2, B5.У3, Д2.У1) – Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації;

– (РН-11)(A1.34, B2.37, B1.32, B5.31, B5.31, B5.32, Д1.34, A1.У1, A1.У4, A2.У5, B1.У1, B1.У1, B2.У3, B5.У3) – Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації;

– (РН-12)(A1.37, A2.36, B2.32, B3.31, A1.У4, A2.У2, B3.У1, B3.У1, Г2.У2, B5.У3) – 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;

– (РН-13)(A3.31, A3.32, A3.36, B2.36, Д1.31, Г2.31, A1.У4, A2.У2, A3.У4, A3.У5, B1.У1, B2.У1, B3.У1, B3.У3) – 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;

– (РН-14)(A1.35, A2.31, Г1.33, A1.У1, A1.У4, A2.У2, A3.У1, B3.У1, Г1.У1, Г2.У2, Г1.У5) – Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів у сфері інформаційної та/або кібербезпеки в цілому;

– (РН-16)(A1.35, B1.31, Г1.33, Д1.32, Д2.32, A1.У1, B1.У1, B1.У4, B3.У1, B4.У2, Д1.У3, Д2.У3) – Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень;

– (РН-18)(A1.36, Е1.33, Д1.33, Д2.32, A1.У3, A3.У5, Г1.У1, Г1.У3, Г2.У4, Е1.У3, Д2.У5) – Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та/або кібербезпеки.

5. Програма навчальної дисципліни

Модуль 1

Змістовий модуль 1. Теоретичні основи менеджменту інформаційної безпеки

Тема 1. Система нормативно-правового регулювання суспільних відносин в інформаційній сфері. [3]: с.18-35, 142-188, 568-583; [4]; [6]: с.9-39, 71-126; [7]: с.44-47, 49-54, 170-191; [8-85]; [93]: с.112-127, [99]; [104]: с.4-22, 38-48; [105]: с.2-36; [106-137]; [142]: с.21-33

Тема 2. Загальні принципи внутрішньої й зовнішньої політики держав у сфері інформаційних відносин. [5]: с.170-179; [10]; [14]; [15]; [19-33]; [35]; [39]; [40]; [53]; [61]; [63-65]; [81]; [93]: с.161-199; [98]: с.539-581; [99]; [104]: с.73-136

Тема 3. Діяльність спеціалізованих міжнародних організацій у сфері інформаційної безпеки. [6]: с.39-69; [34]; [78]; [104]: с.23-37, 49-59

Змістовий модуль 2. Методики менеджменту інформаційної безпеки

Тема 5. Управління інформаційною безпекою на рівні постачальників інформаційних систем. [6]: с.345-364; [104]: с.60-72; [125]

Тема 6. Менеджмент інформаційної безпеки на рівні підприємств. [3]: с.512-567; [6]: с.240-381; [7]; [9]; [14-16]; [62]; [66-71]; [77]; [79]; [82-85]; [104]: с.137-225; [105]: с.37-96, 128-215; [134]

Тема 7. Методики оцінювання ефективності систем захисту інформації. [1]: с.182-207; [2]; [3]: с.78-139, 544-552; [6]: с.121-125, 141-232, 383-406; [36-39]; [41-60]; [80]; [86-91]; [93]: с.131-140; [105]: с.96-127; [137]; [142]: с.33-416

Тема 8. Програмні засоби підтримки менеджменту інформаційної безпеки. [6]: с.141-232; [142]: с.33-105, 368-391, 395-396, 407-430

Тематичний план навчальної дисципліни

Назви змістових модулів і тем	Денна форма				Заочна форма			
	Кількість годин							
	усього	у тому числі			усього	у тому числі		
		л	лаб	с.р		л	лаб	с.р
Модуль 1								
Змістовий модуль 1. Теоретичні основи менеджменту інформаційної безпе								
Тема 1. Система нормативно-правового регулювання суспільних відносин в інформаційній сфері.	10	2	2	6	10	2	2	6
Тема 2. Загальні принципи внутрішньої й зовнішньої політики держав у сфері інформаційних відносин.	4	2	-	2	4		-	4
Тема 3. Діяльність спеціалізованих міжнародних організацій у сфері інформаційної безпеки.	6	2	-	4	6		-	6
Тема 4. Критерії оцінки ефективності систем інформаційної безпеки	10	2	2	6	10		-	10
Разом за змістовим модулем 1	30	8	4	18	30	2	2	26
Змістовий модуль 2. Методики менеджменту інформаційної безпеки								
Тема 5. Управління інформаційною безпекою на рівні постачальників інформаційних систем.	8	2	-	6	8	2	-	6
Тема 6. Менеджмент інформаційної безпеки на рівні підприємств.	14	2	2	10	14		2	12
Тема 7. Методики оцінювання ефективності систем захисту інформації.	30	2	8	20	30		4	22
Тема 8. Програмні засоби підтримки менеджменту інформаційної безпеки	8	1	1	6	8		-	12

Назви змістових модулів і тем	Денна форма				Заочна форма			
	Кількість годин							
	усього	у тому числі			усього	у тому числі		
		л	лаб	с.р		л	лаб	с.р
Разом за змістовим модулем 2	60	7	11	42	60	2	6	52
Разом	90	15	15	60	90	4	8	78

Для студентів заочної форми навчання читаються оглядові лекції за темами змістових модулів в обсягах відповідно до вищенаведеної таблиці.

Теми практичних занять

Практичні роботи програмою не передбачені

Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
Модуль 1		
Змістовий модуль 1		
1	Нормативно-правова база менеджменту інформаційної безпеки	2
2	Методика КПП для оцінювання ефективності систем захисту інформації	2
Разом за змістовим модулем 1		4
Змістовий модуль 2		
3	Менеджмент інформаційної безпеки на об'єктах критичної інфраструктури	2
4	Методики оцінювання ефективності систем захисту інформації на основі ризиків: OCTAVE, NIST, FAIR, MESARI, IRAM	2
5	Метод оцінювання ефективності систем захисту інформації на основі логіко-лінгвістичного підходу	2
6	Методика оцінювання ефективності систем захисту інформації на основі логіко-ймовірнісного підходу	2
7	Інвестиції в інформаційну безпеку	2
8	Порівняльний аналіз методів і програмних засобів оцінювання ефективності систем захисту інформації	1
Разом за змістовим модулем 2		11
Разом		15

Студенти заочної форми виконують роботи № 1, 3, 4, 7,

Самостійна робота

Самостійна робота здобувача вищої освіти є однією з форм організації

навчання, основною формою оволодіння навчального матеріалу в час, вільний від обов'язкових навчальних занять.

Метою самостійної роботи є повторення й осмислення студентом основних питань кожної теми, висвітлених на лекційних і лабораторних заняттях. Самостійна робота проводиться в лабораторіях НУК, читальних залах, на об'єктах майбутньої діяльності і/або вдома. Результати цієї роботи фіксуються студентом в індивідуальному робочому зошиті (конспекті).

Навчальний матеріал дисципліни, передбачений для засвоєння здобувачем вищої освіти в процесі самостійної роботи, виноситься на підсумковий контроль поряд з навчальним матеріалом, який опрацьовувався при проведенні навчальних занять.

Розподіл годин самостійної роботи для денної форми навчання:

- підготовка до лекційних занять – 0,5 год. / 1 заняття (на 1 лекцію);
- самостійне опрацювання окремих тем навчальної дисципліни (які не викладаються на лекціях) – 2 год. / 1 заняття;
- підготовка до лабораторних занять – 1-2 год. / 1 заняття;
- підготовка до модульних контрольних робіт 5 год на 1 роботу
- підготовка до екзаменів – 22 год. на 1 захід.

Розподіл годин самостійної роботи для заочної форми навчання:

- підготовка до лекційних занять – 2 год. / 1 заняття (на 1 лекцію);
- самостійне опрацювання окремих тем навчальної дисципліни (які не викладаються на лекціях) – 4 год. / 1 заняття;
- підготовка до лабораторних занять – 2 год. / 1 заняття;
- підготовка до модульних контрольних робіт 5 год на 1 роботу
- підготовка до екзаменів – 22 год. на 1 захід.

Розподіл годин самостійного опрацювання окремих тем навчальної дисципліни

№ з/П	Назва теми	Кількість годин	
		Д.Ф.Н	З.Ф.Н.
Модуль 1			
1	До теми 1. Зміни у нормативно-правовому забезпеченні менеджменту інформаційної безпеки за останні два роки	2	1
2	До теми 2. Стратегія кібербезпеки України і план її реалізації	2	1
3	До теми 3. Сучасні міжнародні стандарти з управління інформаційною безпекою	2	2
4	До теми 4. Порівняльний аналіз ймовірнісних критеріїв і критеріїв на основі ризиків	2	3
5	До теми 5. Вбудовані моделі інформаційної безпеки провідних постачальників програмних продуктів підтримки прийняття рішень в галузі менеджменту інформаційної безпеки.	2	2

№ з/п	Назва теми	Кількість годин	
		Д.Ф.Н	З.Ф.Н.
6	До теми 6. Управління інформаційною безпекою на транспорті	2	2
7	До теми 7. Ефективність інформаційної боротьби	2	1
8	До теми 8. Програмні засоби оцінювання ефективності політики безпеки	2	1
Разом		16	41

Розподіл годин підготовки самостійної роботи

№	Вид роботи	Кількість годин	
		ДФН	ЗФН
Модуль 1			
1	Підготовка до лекцій	4	4
2	Підготовка до лабораторних робіт	8	8
3	Підготовка до модульних контрольних робіт	10	10
4	Самостійне опрацювання окремих тем навчальної дисципліни	16	16
5	Підготовка до екзамену	22	22
Разом за курсом		60	78

Індивідуальне науково-дослідне завдання

Індивідуальне навчально-дослідне програмою не передбачене.

6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування

Здобувач зобов'язаний вивчити теоретичний матеріал та здобути практичні навички у відповідності до тематичного плану навчальної дисципліни.

Методами навчання є:

- пояснення, демонстрування;
- лекція; відеометод;
- робота з літературою;
- лабораторна робота;
- інструктаж (інструктаж з техніки безпеки та пожежної безпеки проводиться одноразово на першому занятті в лабораторії);
- репродуктивний метод;
- метод проблемного викладу.

При вивченні дисципліни використовуються 3 групи методів навчання:

I група методів - методи організації та здійснення навчально-пізнавальної діяльності:

- словесні: розповідь-пояснення, лекція;

- наочні: ілюстрація, презентація, демонстрація;
- практичні: лабораторні роботи;
- індуктивні методи: узагальнення, пов'язані із проведенням експериментів;
- дедуктивні методи: розвиток абстрактного мислення для засвоєння навчального матеріалу на основі узагальнень;
- репродуктивні методи: робота за готовими прикладами;
- творчі, проблемно-пошукові методи: самостійна, творча пізнавальна діяльність;
- навчальна робота студентів під керівництвом НПП;
- самостійна робота студентів.

II група методів - методи стимулювання й мотивації навчально-пізнавальної діяльності:

- методи стимулювання інтересу до навчання: створення ситуації інтересу при викладанні матеріалу; аналіз життєвих ситуацій;
- методи стимулювання обов'язку й відповідальності: роз'яснення мети навчального предмета; вимоги до вивчення предмета; заохочення та покарання в навчанні;

III група методів - методи контролю (самоконтролю, взаємоконтролю), корекції (самокорекції, взаємокорекції) за ефективністю навчально-пізнавальної діяльності:

Засобами оцінювання результатів навчання є:

- модульні контрольні роботи;
- звіти з лабораторних робіт;
- командні проєкти;
- індивідуальні та групові завдання;
- завдання на лабораторному обладнанні;
- екзаменаційні роботи;
- комплексна контрольна робота (за необхідністю).

Методами демонстрування результатів навчання є:

- усні відповіді;
- письмові відповіді;
- виконання завдань із застосуванням комп'ютерної техніки;
- оформлення звітів з лабораторних робіт;
- презентації результатів виконаних завдань та досліджень.

Допускається застосування дистанційних технологій для діагностики результатів навчання.

7. Форми поточного та підсумкового контролю

Досягнення здобувача вищої освіти оцінюються за 100-бальною системою Університету.

Поточний контроль проводиться в межах навчальних занять і передбачає оцінювання теоретичної підготовки здобувачів вищої освіти із зазначених тем (у тому числі, самостійно опрацьованого матеріалу) та практичних навичок, набутих під час виконання лабораторних робіт.

Поточний контроль здійснюється протягом семестру в наступних формах:

- перевірка екзаменаційних робіт;
- перевірка та захист звітів з лабораторних робіт;
- проведення та перевірка модульних контрольних робіт;
- контрольна робота на заочній формі навчання;
- семестрова атестація;
- перевірка конспекту лекцій;
- контроль відвідування занять.

Перевірка звіту з лабораторної роботи включає оцінювання правильності та повноти виконання завдання, правильності та повноти висновків, правильності оформлення звіту.

Процедура захисту звіту з лабораторної роботи включає один або декілька елементів:

- письмове викладення відповідей на запитання за тематикою роботи;
- усне опитування за тематикою роботи;
- виконання завдань із застосуванням комп'ютерної техніки.

При виконанні модульних контрольних робіт здобувач вищої освіти відтворює засвоєні знання шляхом надання письмових відповідей на поставлені запитання. На теоретичні запитання необхідно давати розгорнуті відповіді, супроводжуючи їх прикладами та ілюстраціями. Повнота відповідей оцінюється згідно з теоретичним матеріалом, наведеним у джерелах інформації для кожної теми. На тестові запитання потрібно вказати номер правильної відповіді та її формулювання.

Контрольна робота на заочній формі навчання за змістом є об'єднаним представленням модульних контрольних робіт, які проводяться для здобувачів денної форми навчання, і має відповідати тим самим вимогам. Контрольна робота на заочній формі навчання виконується протягом семестру і здається до проведення підсумкового контролю.

Поточний модульний контроль проводиться з урахуванням даних поточного контролю за відповідний змістовний модуль і має на меті оцінку

результатів знань студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля.

Семестрова атестація дає змогу здійснити проміжну оцінку досягнень здобувача вищої освіти. В період семестрової атестації викладач оцінює результати поточного контролю та атестує чи не атестує здобувача вищої освіти.

За рішенням кафедри студентам, які брали участь у науково-дослідній роботі – роботі конференцій, студентських наукових гуртків, підготовці публікацій, а також були учасниками олімпіад, конкурсів, тощо можуть присуджуватися додаткові бали. Додаткові бали також можуть присуджуватися за результатами перевірки конспекту лекцій, контролю відвідування занять та за активність на лекціях і практичних заняттях.

За всі поточні контрольні заходи протягом семестру, з урахуванням додаткових балів, студент сумарно може отримати від 0 до 100 балів.

Умовою допуску студента до семестрового підсумкового контролю є мінімальна сума у 60 балів, яку студент повинен набрати у разі виконання всіх елементів модулів.

Семестровий підсумковий контроль з дисципліни проводиться відповідно до навчального плану у вигляді **екзамену** в терміни, встановлені графіком навчального процесу, та в обсязі навчального матеріалу, визначеному робочою програмою навчальної дисципліни.

Студент, який набрав за всі поточні контрольні заходи менше 60 балів або хоче отримати додаткові бали, пише семестрову екзаменаційну роботу (проводиться у письмовій формі), до якої він допускається, якщо він має за виконання всіх передбачених елементів модулів не менше 35 балів. Максимальна кількість балів за семестрову підсумкову залікову роботу (екзамен) становить 40 балів. Студенти заочної форми навчання пишуть підсумкову залікову роботу обов'язково.

Підсумкова оцінка з дисципліни від 60 до 100 балів визначається як сума балів за змістовими модулями та семестрової залікової роботи (у разі її написання).

Зарахування кредитів навчального курсу можливо тільки після досягнення результатів, запланованих РПНД, що виражається в одній з позитивних оцінок, передбачених чинним законодавством.

8. Критерії оцінювання результатів навчання

8.1 Критерії оцінювання лабораторних робіт

При оцінюванні лабораторних робіт враховуються наступні критерії:

- виконання роботи та правильність виконання;
- наявність звіту, вчасність подачі та якість звіту;
- захист звіту.

Максимальна оцінка за кожну лабораторну роботу для студентів ДФН становить 5 балів.

Максимальна оцінка за кожну лабораторну роботу для студентів ЗФН становить 8 балів.

Максимальна сумарна кількість балів за лабораторні роботи для студентів ДФН становить: $8 \times 5 = 40$ балів

Максимальна сумарна кількість балів за лабораторні роботи для студентів ЗФН становить: $8 \times 4 = 32$ бали.

Критерії оцінювання лабораторних робіт

Кількість балів (в дужках для ЗФН)	Критерії оцінювання
Модуль 1	
5 (8)	Роботу виконано самостійно, завдання виконано правильно. Звіт здано у встановлений термін, оформлення звіту повністю відповідає вимогам, у висновках проведено коректну інтерпретацію результатів. Студент надав правильні відповіді на всі питання захисту.
4 (6,4)	Робота виконана правильно з консультаціями викладача. Звіт здано у встановлений термін, можливі несуттєві помилки в оформленні звіту та незначні некоректності у висновках. Студент надав принципово правильні відповіді на питання захисту (без суттєвих помилок).
3 (4,8)	Роботу виконано із підказками викладача та незначними помилками. Звіт містить неточності у висновках та окремі помилки. Студент відповів на питання захисту частково чи з принциповими помилками.
2 (3,2)	Завдання виконано у повному об'ємі але з помилками. Звіт містить неточності у висновках та окремі помилки. Студент не відповів на питання захисту.
1 (1,6)	Завдання виконано не у повному об'ємі (не менше 70%). Надано звіт, що містить неточності і помилки. Студент не відповів на питання захисту.
0 (0)	Робота не виконана.
	<i>Максимальна сумарна оцінка студента за даний компонент програми для ДФН – 40 балів (8 робіт по 5 балів). Максимальна сумарна оцінка студента за даний компонент програми для ЗФН – 32 балів (4 роботи по 8 балів). При незначних відхиленнях від вказаних критеріїв оцінка може доповнюватись знаками «-» або «+», що при підсумовуванні відповідає 0,5 бала.</i>

8.2 Критерії оцінювання модульних контрольних робіт

Для поточного модульного контролю студентами виконуються 2 (дві) модульні контрольні роботи (МКР) за матеріалами змістовних модулів.

Критерієм оцінювання МКР є відсоток правильних відповідей на питання модульної контрольної роботи.

Максимальна кількість балів за кожну МКР для студентів ДФН становить 10 балів.

Загальна сума балів за модульні контрольні роботи для студентів ДФН становить: $2 \times 10 = 20$ балів;

Максимальна кількість балів за кожну МКР для студентів ЗФН становить: 14 балів.

Загальна сума балів за модульні контрольні роботи для студентів ЗФН становить: $2 \times 14 = 28$ балів.

Критерії оцінювання задач та практичних завдань в МКР для ДФН

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал	10	9	8	7	6	5	4	3	2	1

Критерії оцінювання задач та практичних завдань в МКР для ЗФН

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал	14	12,6	11,2	9,8	8,4	7,0	5,6	4,2	2,8	1,4

8.3 Критерії оцінювання екзаменаційної роботи

Максимальна оцінка за екзаменаційні роботи – 40 балів.

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал	40	36	32	28	24	20	16	12	8	4

Рівні підсумкової оцінки екзамену з дисципліни

(перерахунковий коефіцієнт – 0,4)

Оцінка за 100-бальною шкалою університету / Grade according to 100-points scale of University	Оцінка за шкалою ЄКТС / Grade according to ECTS scale
90-100 (творчий рівень)/(creative level)	A (відмінно) / (excellent)
82-89 (високий рівень)/(high level)	B (дуже добре) / (very good)
74-81 (добрий рівень)/(good level)	C (добре) / (good)

Оцінка за 100-бальною шкалою університету / Grade according to 100-points scale of University	Оцінка за шкалою ЄКТС / Grade according to ECTS scale
64-73 (середній рівень)/(average level)	D (посередньо) / (average)
60-63 (задовільний рівень)/(satisfactory level)	E (достатньо) / (satisfactory)
35-59 (низький рівень)/(low level)	FX (незадовільно з можливістю повторного складання) / (unsatisfactory with the possibility to repass the exam)
1-34 (незадовільний рівень)/(unsatisfactory level)	F (незадовільно з обов'язковим повторним вивченням) / (unsatisfactory with the compulsory repeating of the course)

8.5 Розподіл балів

Розподіл оцінки за змістовними модулями та видами контролю

		Денна форма		Заочна форма	
		Вид роботи	Кількість балів	Вид роботи	Кількість балів
Модуль 1					
ЗМ1	T1	Лабораторна робота 1	5	Лабораторна робота 1	8
	T4	Лабораторна робота 2	5	-	-
	МКР1	Тест	10	Тест	14
ЗМ2	T6	Лабораторна робота 3	5	Лабораторна робота 3	8
	T7	Лабораторні роботи 4, 5, 6	15	Лабораторна робота 4	8
	T8	Лабораторні роботи 7, 8	10	Лабораторна робота 7	8
	МКР2	Тест	10	Тест	14
Підсумковий семестровий контроль		екзамен	40	екзамен	40
Всього			100		100

9. Засоби навчання

Апаратне забезпечення, необхідне для вивчення навчальної дисципліни, включає персональний комп'ютер (настільний або ноутбук) із доступом до Інтернет.

Програмне забезпечення, необхідне для вивчення навчальної дисципліни, включає:

- операційну систему Windows;
- текстовий процесор та редактор растрових зображень (для підготовки звітів з лабораторних робіт);
- pdf-, djv-переглядач (для ознайомлення з джерелами інформації, представленими в електронній формі);
- Power Point для ознайомлення з тематичними презентаціями;
- MS Excel та Mathcad для виконання розрахункових завдань.

Використовуються апаратні та програмні можливості лабораторій №129 і 130, 133 б кафедри КТІБ ННІАЕ НУК.

В процесі проведення лекцій і лабораторних робіт для демонстрації тематичних презентацій і прикладів використовується наявне в лабораторіях мультимедійне обладнання.

10. Рекомендовані джерела інформації

Основна література

Навчально-методична література

1. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект. [Підручник]. / В. Л. Бурячок, В.Б. Толубко, В. О. Хорошко, С.В. Толюпа. – Львів.: «Магнолія 2006», 2018. – 320 с. URL: <https://spadok.org.ua/books/Buryachok-Osnovy-info-ta-ciberbezpeky.pdf>
2. Горохов С.М. Програми та методики державної експертизи інформаційної захищеності телекомунікацій : навч. посіб. / С.М. Горохов, Н. В. Кондратьєва, В.Г. Кононович, С.В. Стайкуца; за ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2013. – 252 с. URL: <https://metod.suitt.edu.ua/download/548>
3. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. - К.: Видавнича група BHV, 2009. – 608 с. URL: https://library.kre.dp.ua/Books/2-4%20kurs/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97/Graivorovskyi_Novikov_Bezpeka_informazino_kommunikat_sistem_2009.pdf
4. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. посібник. - Дніпро: Дніпропетровський держ. ун-т внутріш. справ, 2020. – 144 с. URL: <https://er.dduvs.in.ua/bitstream/123456789/5717/1/%D0%9F%D0%9E%D0%A1%D0%91%D0%9D%D0%98%D0%9A%20%D0%9E%D0%A3%D0%91%20.pdf>
5. Ромака В. А. та ін. Системи менеджменту інформаційної безпеки : навч. посібник. -Львів : Вид-во Львів політехніки, 2012. – 232 с.
6. Корченко О.Г. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с. URL: <http://ir.stu.cn.ua/bitstream/handle/123456789/19244/%D0%9C%D0%B5%D0%BD%D0%B5%D0%B4%D0%B6%D0%BC%D0%B5%D0%BD%D1%82%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC.%20%D0%B1%D0%B5%D0%B7%D0%BF.%20New%20booklet%201.pdf?sequence=1&isAllowed=y>
7. Усік П.С., Буравченко К.О. Безпека банківських систем : навч. посіб. / П. С. Усік, К. О. Буравченко; М-во освіти і науки України, Центральн. нац. техн. ун-т.— Кропивницький: ЦНТУ, 2022. — 194 с. URL: http://dspace.kntu.kr.ua/jspui/bitstream/123456789/12094/3/%D0%9D%D0%B0%D0%B2%D1%87%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA_%D0%91%D0%91%D0%A1_2.pdf

Нормативно-правова база

Закони України:

8. Доктрина інформаційної безпеки України. URL: <https://www.president.gov.ua/documents/472017-21374>
9. Закон України «Про банки і банківську діяльність». URL: <http://zakon2.rada.gov.ua/laws/show/2121-14>.
10. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України». URL: <http://zakon2.rada.gov.ua/laws/show/3475-15>.
11. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»/ URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>

12. Закон України «Про захист персональних даних» URL: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2297-17>
13. Закон України «Про інформацію». URL: <http://zakon2.rada.gov.ua/laws/show/2657-12>.
14. Закон України "Про критичну інфраструктуру". URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>
15. Закон України „Про ліцензування певних видів господарської діяльності”. URL: <https://zakon.rada.gov.ua/laws/show/222-19#Text>
16. Закон України «Про Національний банк України». URL: <http://zakon3.rada.gov.ua/laws/show/679-14>.
17. Закон України «Про платіжні системи та переказ коштів в Україні». URL: <http://zakon3.rada.gov.ua/laws/show/2346-14/ed20120527>
18. Закон України «Про основні засади забезпечення кібербезпеки України» URL: <http://zakon.rada.gov.ua/laws/show/2163-19>
19. План реалізації стратегії кібербезпеки України URL: <https://zakon.rada.gov.ua/laws/show/n0087525-21#Text>
20. Стратегія кібербезпеки України URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>
21. Указ Президента України від 27.09.99 № 1229 “Про затвердження Положення про технічний захист інформації в Україні”. URL: <https://zakon.rada.gov.ua/laws/show/1229/99#Text>

Постанови Кабінету міністрів України

22. Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури, затверджені постановою Кабінету Міністрів України № 518 від 19.06.2019. URL: <https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#n8>
23. Методика категоризації об’єктів критичної інфраструктури, затверджена Постановою Кабінету міністрів України №1109 від 9.10.2020. URL: <https://zakon.rada.gov.ua/rada/show/1109-2020-%D0%BF#Text>
24. Перелік секторів (підсекторів), основних послуг критичної інфраструктури держави, затверджений Постановою Кабінету міністрів України №1109 «Деякі питання об’єктів критичної інформаційної інфраструктури» від 9.10.2020. URL: <https://zakon.rada.gov.ua/rada/show/1109-2020-%D0%BF#Text>
25. Положення про організаційно-технічну модель кіберзахисту, затверджене Постановою Кабінету міністрів України №1426 від 29.12.2021. URL: <https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text>
26. Порядок віднесення об’єктів до об’єктів критичної інфраструктури, затверджений Постановою Кабінету міністрів України №1109 від 9.10.2020. URL: <https://zakon.rada.gov.ua/rada/show/1109-2020-%D0%BF#Text>
27. Порядок пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, затверджений Постановою Кабінету міністрів України №497 від 16.05.2023. URL: <https://zakon.rada.gov.ua/laws/show/497-2023-%D0%BF#Text>
28. Порядок реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджений Постановою Кабінету міністрів України №299 від 04.04.2023. URL: <https://www.kmu.gov.ua/storage/app/uploads/public/642/d7c/c11/642d7cc11ad3b844545241.doc>
29. Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, затверджений Постановою Кабінету міністрів України №1295 від 23.12.2020. URL: <https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF>
30. Постанова Кабінету міністрів України «Деякі питання об’єктів критичної інформаційної інфраструктури» № 943 від 9.10.2020.. URL: <https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#n16>
31. Постанова Кабінету міністрів України «Деякі питання об’єктів критичної інфраструктури» №1109 від 9.10.2020. URL: <https://zakon.rada.gov.ua/rada/show/1109-2020-%D0%BF#Text>

32. Постанова Кабінету міністрів України «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» №299 від 04.04.2023. URL: <https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text>

33. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені Постановою Кабінету Міністрів України № 373 від 29.03.06. URL: <https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text>

Міжнародні нормативні документи

34. Директива Європейського Парламенту та Ради (ЄС) 2016/1148 від 06.07.2019 "Про заходи високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу". URL: https://zakon.rada.gov.ua/rada/show/984_013-16#n3

35. Директива Ради 2008/114/ЄС від 08.12.2008 "Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту". URL: https://zakon.rada.gov.ua/rada/show/984_002-08#n4

36. CSC-STD-001-83. Trusted Computer System Evaluation Criteria. URL: <https://www.cs.cmu.edu/afs/cs/usr/bsy/security/CSC-STD-001-83.txt>.

37. CSC-STD-003-85 Guidance for applying the Department of Defence Trusted Computer System Evaluation Criteria in specific environment. URL: http://www.cbi.umn.edu/securitywiki/pub/CBI_ComputerSecurity/PubRainbowSeries/csc-std-003-85lightyellow.pdf

38. CTCPEC. Canadian Trusted Computer Product Evaluation Criteria. URL: http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio_kanadskie_kriterii_bezopasnosti_kompjuternyx_sistem_ctcpec.

39. Cybersecurity Capacity Maturity Model for Nations. URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=57945> Модель зрілості потенціалу кібербезпеки для націй

40. ETSI GS ISI 007 V 1.1 (2018-12) Guidelines for building and operating a secured Security Operations Center (SOC). URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=57941> Вказівки щодо побудови та експлуатації захищеного операційного центру безпеки (SOC)

41. Information Technology Security Evaluation Criteria URL: https://www.bsi.bund.de/shareddocs/downloads/de/bsi/zertifizierung/interpretationen/ais_18_itsec_jil_e_pdf.pdf?_blob=publicationfile.

42. ISO/IEC 9001:2000 Quality management systems. Requirements. URL: <https://www.iso.org/standard/21823.html>.

43. ISO/IEC 14001:2015 Environmental management systems. Requirements with guidance for use. URL: <https://www.iso.org/standard/60857.html>

44. ISO/IEC 15408-1:2009. Informational technology. Security techniques. Evaluation criteria for IT security. Part 1: Introduction and general model. URL: <https://www.iso.org/standard/50341.html>

45. ISO/IEC 15408-2:2008. Informational technology. – Security techniques – Evaluation criteria for IT security. – Part 2: Security functional requirements. URL: <https://www.iso.org/standard/46414.html>

46. ISO/IEC 15408-3:2008. Informational technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirement. URL: <https://www.iso.org/standard/46413.html>

47. ISO/IEC 17799:2005. Information technology. Security techniques. Code of practice for information security management. URL: <https://www.iso.org/standard/39612.html>.

48. ISO/IEC 18045:2005. Informational technology – Security techniques – Methodology for IT security evaluation.

49. ISO/IEC 27001:13. Information technology. Security techniques. Information security management systems. Requirements. URL: <https://www.iso.org/standard/54534.html>.

50. ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls. URL: <https://www.iso.org/ru/standard/54533.html>

51. ISO 27005:2018 Information technology -- Security techniques -- Information security risk management. URL: <https://www.iso.org/standard/75281.html>

52. Federal Information Processing Standards. URL: <http://csrc.nist.gov/publications/PubsFIPS.html>.
53. National Capabilities Assessment Framework. URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=57942> Керівництво з оцінки національних спроможностей
54. NCSC-TG-001A Guide to Understanding Audit in Trusted Systems. URL: <https://fas.org/irp/nsa/rainbow/tg001.htm>.
55. NCSC-TG-003A guide to understanding discretionary access control in trusted systems. URL: <http://csrc.nist.gov/publications/secpubs/rainbow/tg003.txt>.
56. NCSC-TG-005 Trusted Network Interpretation. URL: <http://www.filewatcher.com/m/NCSC-TG-005.pdf.1290550-0.html>.
57. NCSC-TG-006-88 Guide to understanding configuration management in trusted systems. URL: <https://fas.org/irp/nsa/rainbow/tg006.htm>.
58. NCSC-TG-007-95A Guide to Understanding Design Documentation in Trusted. URL: <http://ftp.mirrorservice.org/sites/ftp.wiretapped.net/pub/security/info/reference/rainbow-books/NCSC-TG-007.pdf>.
59. NCSC-TG-021 Trusted Database Management System Interpretation. URL: http://www.cbi.umn.edu/securitywiki/pub/CBI_Computer_Security/PubRainbow_Series/ncsc-tg-021purple.pdf.
60. NIST (SP) 800-61 Computer Security Incident Handling Guide. URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=57944> Керівні настанови щодо управління інцидентами, пов'язаними з комп'ютерною безпекою

Нормативні документи системи ТЗІ України

61. Методичні рекомендації з розроблення публічної пропозиції про здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, затверджені Наказом Адміністрації Держспецзв'язку №599 від 14.07.2023. URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=54465>
62. Методичні рекомендації щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами, затверджені Наказом Адміністрації Держспецзв'язку №463 від 29.05.2023. URL: <https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-29-05-2023-463-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-zabezpechennya-kiberzakhistu-avtomatizovanih-sistem-upravlinnya-tekhnologichnimi-procesami>
63. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджені Наказом Адміністрації Держспецзв'язку №601 від 06.10.2021. URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=50156>
64. Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджені Наказом Адміністрації Держспецзв'язку №570 від 03.07.2023. URL: <https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-03-07-2023-570-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-reaguvannya-sub-yektami-zabezpechennya-kiberbezpeki-na-rizni-vidi-podii-u-kiberprostori>
65. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури» №23 від 15.01.2021. URL: <https://zakon.rada.gov.ua/rada/show/v0023519-21#Text>
66. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. URL: <https://tzi.com.ua/downloads/1.4-001-2000.pdf>
67. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. URL: <http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106342>
68. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. URL: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?jsessionid=afd6198c23cb1f96abafd7189bbdce03?showhidden=1&art_id=101870&cat_id=89734&ctime=1344501089407.

69. НД ТЗІ 2.5-008-02 "Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2". URL: <http://info-stand.com/nb-ukraine/by-type/nd-tzi/22-ndtzi25-008-02.html>.

70. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. URL: <http://www.dsszzi.gov.ua/%2fdstszi/%2fdoccatalog/%2f document %3fid%3d41647&ei=guz5uk3xg8zsga4r4cwcq&usg=afqjcnfy5kjfdqsympy-ekqedagtercmw&cad=tja>.

71. НД ТЗІ 2.6-001-11 «Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах». URL: <http://dstszi.kmu.gov.ua/dstszi/doccatalog/document;jsessionid=62556e8a1a8a5363657e5da67bfce233?id=103245>

72. НД ТЗІ 2.6-002-2015 Порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=89740.

73. НД ТЗІ 2.6-003-2015 Порядок зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=89740.

74. НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу. URL: <http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=103246>.

75. НД ТЗІ 2.7-010-09. Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу. URL: <https://tzi.com.ua/downloads/2.7-010-09.pdf>

76. НД ТЗІ 2.7-013-2016 Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=89740.

77. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі». URL: <https://tzi.com.ua/downloads/3.7-003-2005.pdf>

78. Організація реагування на інциденти та обробка інцидентів безпеки: Керівництво для організації електрозв'язку. Рекомендація МСЭ-Т Е.409 (ITU-Т Е.409). – Женева, 2004. URL: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.409-200405-I!!PDF-E&type=items

79. Положення про захист електронних банківських документів з використанням засобів захисту інформації Національного банку України. URL: <http://bank.gov.ua/doccatalog/document?id=22694128>.

80. Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджений Наказом Адміністрації Держспецзв'язку №660 від 02.12.2014. URL: <https://zakon.rada.gov.ua/laws/show/z0090-15#n14>

81. Порядок сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті, затверджений Наказом Адміністрації Держспецзв'язку №20 від 15.01.2016. URL: <https://zakon.rada.gov.ua/laws/show/z0196-16#n13>

82. Правила організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України. URL: <http://zakon2.rada.gov.ua/laws/show/z0419-07>.

83. Р–СП Рекомендації з технічного захисту інформації в приміщеннях серверних, електронної пошти та інших спеціальних приміщень. - К.:ТОВ "НікС", 2003. - 25 с.

84. СОУ Н НБУ 65.1 СУІБ 1.0:2010 «Методи захисту в банківській діяльності, система управління інформаційною безпекою. Вимоги»/ URL: <http://www.bank.gov.ua/doccatalog/document?id=72235>.

85. СОУ Н НБУ 65.1 СУІБ 2.0:2010 «Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою» URL: <https://kyianyn.files.wordpress.com/2010/12/nbu-27002.pdf>.

86. Архіпов А.Є, Архіпова Є.О. Особливості визначення обсягу інвестицій в систему захисту інформаційних ресурсів // Інвестиції: практика та досвід. – 2015/ - № 11. – С.71-74. URL: http://www.investplan.com.ua/pdf/11_2015/16.pdf

87. Василенко В.С., Бордюк О.С., Полонський С.М. Оцінювання ризиків безпеки інформації в локальних обчислювальних мережах. [URL]: http://www.rusnauka.com/11_EISN_2010/Informatica/64068.doc.htm

88. Верескун М.В. Ефективність інвестицій в інформаційну безпеку: проблеми і рішення // Вісник Приазовського державного технічного університету. Серія : Економічні науки. - 2015. - Вип. 30. - С. 220-227. [URL}: http://nbuv.gov.ua/UJRN/VPDTU_ek_2015_30_30

89. Домарев В.В. Система моніторингу стану національної безпеки в інформаційній сфері на основі моделі комплексної оцінки з використанням інтегрованих показників //Захист інформації. – 2005. – Т.7 - №1(22) URL: <https://jrnل.nau.edu.ua/index.php/ZI/article/view/3832>

90. Дудикевич В.Б., Микитин Г.В., Крет Т.Б. Концепція та базовий підхід до побудови системи захисту інформації в багаторівневій інтелектуальній системі керування //Системи обробки інформації, 2016, випуск 8 (145). - С.105-110. URL: https://www.hups.mil.gov.ua/periodic-app/article/16975/soi_2016_8_24.pdf

91. Левченко Е.Г., Прус Р.Б., Рабчун Д.І. Показники продуктивності витрат на захист інформації //Безпека інформації. - 2012.- №2(18). - С.6-11. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/bezin_2012_2_3.pdf

Допоміжна література

Навчально-методична література

92. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. /В.Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний Н.В. Лукова-Чуйко. – К.: ДУТ-КНУ, 2016. – 178 с. URL: https://duikt.edu.ua/uploads/p_303_32151446.pdf?file=p_303_32151446.pdf

93. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. /В.Л. Бурячок, Р.В. Киричок, П.М. Складанний. – К., 2019. – 320 с. URL: https://elibrary.kubg.edu.ua/id/eprint/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf

94. Гапак О. М., Глебена М. І. Захист інформації в комп'ютерних системах. – Ужгород: УЖНУ, 2021. – 184 с. URL: https://dSPACE.uzhnu.edu.ua/jspui/bitstream/lib/36506/1/%D0%9F%D0%86%D0%94%D0%A0%D0%A3%D0%A7%D0%9D%D0%98%D0%9A%D0%97%D0%86%D0%9A%D0%A1_2021.pdf

95. Голубів В. О., Гавловський В. Д., Цимбалюк В. С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій : навч. посібник. -Запоріжжя : ГУ "ЗІДМУ", 2002. – 292 с.

96. Домарев В.В., Домарев Д.В. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k) – Донецьк: Велстар, 2012. – 146 с.

97. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2017. Частина 13: Захист інформації в системах електронного урядування / [О.М. Хошаба]. – К.: ФОП Москаленко О. М., 2017. – 72 с. URL: https://iq.vntu.edu.ua/fdb/1124/publications/146_Khoshaba_pidruchnik.pdf

98. Єсін В. І., Кузнецов О. О., Сорока Л. С. Безпека інформаційних систем і технологій: навчальний посібник [для студентів вищих навчальних закладів, які навчаються за напрямом підготовки «Безпека інформаційних і комунікаційних систем»] / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х. : ХНУ імені В. Н. Каразіна, 2013. – 632 с. URL: https://library.kre.dp.ua/Books/2-4%20kurs/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97%D0%84%D1%81%D1%96%D0%BD_%D0%92.%D0%86._%D0%91%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%

B0_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D1%85_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC_%D1%96_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D0%B9_%D0%A5%D0%B0%D1%80%D0%BA%D1%96%D0%B2_2013.pdf

99. Знахур С. В. Інформаційний менеджмент та маркетинг : конспект лекцій. – Харків: Вид. ХНЕУ, 2009. – 132 с. URL: <http://www.repository.hneu.edu.ua/bitstream/123456789/3110/1/%d0%9a%d0%be%d0%bd%d1%81%d0%bf%d0%b5%d0%ba%d1%82%20%d0%bb%d0%b5%d0%ba%d1%86%d1%96%d0%b9.%20%d0%86%d0%bd%d1%84%d0%be%d1%80%d0%bc%d0%b0%d1%86%d1%96%d0%b9%d0%bd%d0%b8%d0%b9%20%d0%bc%d0%b5%d0%bd%d0%b5%d0%b4%d0%b6%d0%bc%d0%b5%d0%bd%d1%82%20%d1%82%d0%b0%20%d0%bc%d0%b0%d1%80%d0%ba%d0%b5%d1%82%d0%b8%d0%bd%d0%b3.%20%d0%97%d0%bd%d0%b0%d1%85%d1%83%d1%80%20%d0%a1.%20%d0%92..pdf>

100. Карачка А.Ф. Технології захисту інформації: Текст лекцій. – Тернопіль: ТНЕУ, 2017. – 86 с. URL: <http://dspace.wunu.edu.ua/retrieve/52646/lekzii.pdf>.

101. Кукарін О.Б. Електронний документообіг та захист інформації: Навчальний посібник. -К.: НАДУ, 2015. – 84 с. URL: https://duikt.edu.ua/uploads/l_1504_14216152.pdf

102. Левченко Є.Г., Швець В. А., Демчишин М.В. Економіка інформаційної безпеки: Навчальний посібник. – К.: НАУ, 2012. – 225 с. [URL]: https://er.nau.edu.ua/bitstream/NAU/10221/1/Ekonom_bezp.pdf

103. Логінова Н.І., Дробожур Р.Р. Правовий захист інформації: Навчальний посібник. - Одеса: Фенікс, 2015. – 264 с. URL: <http://dspace.onua.edu.ua/bitstream/handle/11300/1824/%D0%9F%D1%80%D0%B0%D0%B2%D0%BE%D0%B2%D0%B8%D0%B9%20%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97.%20%D0%9B%D0%BE%D0%B3%D1%96%D0%BD%D0%BE%D0%B2%D0%B0%2C%20%D0%94%D1%80%D0%BE%D0%B1%D0%BE%D0%B6%D1%83%D1%80.pdf?sequence=1&isAllowed=y>

104. Носок С.О., Фаль О.М., Ткач В.М. Управління інформаційною безпекою: конспект лекцій [Електронний ресурс]: навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1114 Кбайт). – К.: КПІ ім. Ігоря Сікорського, 2021. – 258 с. URL: https://ela.kpi.ua/bitstream/123456789/43377/1/Konspekt-Lektsii_UIB.docx

105. Якименко І.З. Конспект лекцій з дисципліни «Менеджмент інформаційної безпеки». – Тернопіль, 2019. – 136 с. URL: http://dspace.wunu.edu.ua/bitstream/316497/36025/1/%D0%9C%D0%B5%D0%BD%D0%B5%D0%B4%D0%B6%D0%BC%D0%B5%D0%BD%D1%82_I%D0%91_%D0%AF%D0%BA%D0%B8%D0%BC%D0%B5%D0%BD%D0%BA%D0%BE_%D0%BB%D0%B5%D0%BA%D1%86ii.pdf

Нормативно-правова база

Закони України:

106. Закон України «Про державну таємницю». URL: <http://zakon.rada.gov.ua/laws/show/3855-12>

107. Закон України „Про доступ до публічної інформації”. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>

108. Закон України «Про електронні комунікації». URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text>

109. Закон України „Про оперативно-розшукову діяльність”. URL: <https://zakon.rada.gov.ua/laws/show/2135-12#Text>

110. Закон України «Про основи національної безпеки України» URL: <http://zakon.rada.gov.ua/laws/show/2469-19>

111. Закон України „Про Раду національної безпеки і оборони України”. URL: <https://zakon.rada.gov.ua/go/183/98-%D0%B2%D1%80>

112. Закон України „Про розвідку”. URL: <https://zakon.rada.gov.ua/laws/show/912-20#Text>

113. Закон України „Про службу безпеки України”. URL: <https://zakon.rada.gov.ua/laws/show/2229-12#Text>

114. Закон України „Про Службу зовнішньої розвідки України”. URL: <https://zakon.rada.gov.ua/laws/show/3160-15#Text>

115. Закон України «Про технічні регламенти та оцінку відповідності». URL: <http://zakon.rada.gov.ua/laws/show/124-19>.

116. Звід відомостей, що становлять державну таємницю URL: <https://zakon.rada.gov.ua/laws/show/z0052-21#Text>

Постанови Кабінету міністрів України:

117. Порядок формування переліку об'єктів критичної інформаційної інфраструктури, затверджений Постановою Кабінету Міністрів України від 9 жовтня 2020 р. № 943. URL: <https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#n16>

118. Порядок внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування, затверджений Постановою Кабінету Міністрів України від 9 жовтня 2020 р. № 943. URL: <https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#n61>

Міжнародні нормативні документи

119. Конвенція про кіберзлочинність: Конвенція Ради Європи від 23.11.01 р. № 994-575. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

120. How to set up CSIRT and SOC. URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=57943> Як налаштувати роботу CSIRT (команда реагування на інциденти комп'ютерної безпеки) та SOC (центр операційної безпеки)

Нормативні документи системи ТЗІ України:

121. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення. URL: <http://metrology.com.ua/download/dstu-gost-gost-r/60-dstu/441-dstu-3396-0-96>.

122. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. URL: <http://metrology.com.ua/download/dstu-gost-gost-r/60-dstu/440-dstu-3396-1-96>.

123. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. URL: <http://www.dut.edu.ua/ru/lib/60/category/925/view/1045>.

124. Наказ Адміністрації Держспецзв'язку «Про затвердження Положення про систему захищеного доступу державних органів до мережі Інтернет» №771 від 30.08.2023. URL: <https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-pro-zatverdzhennya-polozhennya-pro-sistemu-zakhishenogo-dostupu-derzhavnikh-organiv-do-merezhi-internet-vid-30-serpnya-2023-roku-771>

125. Наказ Адміністрації Держспецзв'язку «Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації» №45 від 26.03.2007. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=50825&cat_id=38835

126. НД ТЗІ 1.1-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. URL: http://www.dut.edu.ua/uploads/1_1027_69115427.pdf.

127. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. URL: <http://www.afa.biz.ua/documents/31-infobezopasnot/33-what-is-uncategorised-article?format=pdf>.

128. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. URL: <https://tzi.com.ua/downloads/1.1-003-99.pdf>.

129. НД ТЗІ 1.1-004-2003 Протидія технічним розвідкам. Терміни та визначення. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article%3Bjsessionid=9082A42798BC38188D392292242BFBA2?showHidden=1&art_id=102366&cat_id=89734&ctime=1344587370607.

130. НД ТЗІ 2.5-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту. URL: <http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=103243>
131. НД ТЗІ 2.5-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту. URL: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?showHidden=1&art_id=101820&cat_id=89734&ctime=1344500798284
132. НД ТЗІ 2.5-003-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту. URL: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?showHidden=1&art_id=101836&cat_id=89734&ctime=1344500934167.
133. НД ТЗІ 2.7-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт. -К.:ТОВ "НікС", 1999. – 54 с.
134. НД ТЗІ 2.7-002-99 Методичні вказівки з використання засобів копіювально-розмножувальної техніки. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102299&cat_id=46556&ctime=1344510938381.
135. НД ТЗІ 2.7-008-08 Захист інформації на об'єктах інформаційної діяльності. Вимоги та рекомендації із забезпечення захисту мовної інформації від витоку акустичним та віброакустичним каналами. Методичні вказівки. URL: https://tzi.ua/ua/nd_tz_2.5-008-2002.html.
136. НД ТЗІ 3.7-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова). URL: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?showHidden=1&art_id=102205&cat_id=46556&ctime=1344503878438.
137. Положення про державну експертизу в сфері технічного захисту інформації, затверджене Наказом Адміністрації Держспецзв'язку № 93 від 16.05.2007 із змінами, затвердженими наказом Адміністрації Держспецзв'язку № 567 від 10.10.2012. URL: <http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=105528>.

Наукові публікації

138. Whitman M. Management of information security /M. Whitman, H. Mattord. – Gengage Learning, 2016. – 722 p URL: [http://www.mim.ac.mw/books/Principles%20of%20Information%20Security%20\(%20PDFDrive%20\).pdf](http://www.mim.ac.mw/books/Principles%20of%20Information%20Security%20(%20PDFDrive%20).pdf)
139. Золотар О.О. Інформаційна безпека людини: теорія і практика : монографія. – К.: ТОВ «Видавничий дім «АртЕк», 2018 – 446 с. URL: https://ippi.org.ua/sites/default/files/informaciyna_bezpeka_lyudini_print.pdf
140. Корченко О.Г., Архипов О.Є., Казмірчук С.В. Аналіз та оцінювання ризиків інформаційної безпеки. - К.: ТОВ «Поліграф-Лазурит», 2013. – 275 с. URL: <https://er.nau.edu.ua/bitstreams/608567f9-7c99-4cb1-ba31-bb66bf7c19c0/download>
141. Корченко О.Г., Гнатюк С.О, Казмірчук С.В., Панченко В.М., Мельник С.В. Аудит та управління інцидентами інформаційної безпеки. – К.: Центр навчально-наукових. та науково-практичних видань НА СБ України, 2014. – 190 с. URL: https://er.nau.edu.ua/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf
142. Корченко О.Г., Казмірчук С.В., Ахметов Б.Б., Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія, Київ, ЦП «Компринт», 2017 – 435 с. URL: https://er.nau.edu.ua/bitstream/NAU/40482/1/Monografiya_ukr.pdf

Інформаційні ресурси в Інтернеті

1. Верховна Рада України. Законодавство України. URL: <http://zakon.rada.gov.ua/laws/>
2. Державна служба спеціального зв'язку та захисту інформації. URL: <https://cip.gov.ua/ua>
3. Діяльність Адміністрації Держспецзв'язку у сфері кіберзахисту. URL: <https://cip.gov.ua/ua/statics/cyber-protection>

4. Команда реагування на комп'ютерні надзвичайні події України.
URL: <https://cert.gov.ua/>
5. Нормативна база у сфері ТЗІ URL: <http://altersign.com.ua/korysna-informacija/normatyvna-baza-u-sferi-tzi>
6. Офіційний сайт ISO. URL: <https://www.iso.org/standard>
7. Перелік документів міжнародних організацій та країн-партнерів у сфері кіберзахисту. URL: <https://cip.gov.ua/ua/news/perelik-dokumentiv-mizhnarodnikh-organizacii-ta-krayin-partneriv-u-sferi-kiberzakhistu>
<https://cip.gov.ua/ua/news/perelik-dokumentiv-mizhnarodnikh-organizacii-ta-krayin-partneriv-u-sferi-kiberzakhistu>
8. Портал безпека. URL: <https://www.bezpeka.com/uk/golovna/>
9. Системи онлайн-освіти. URL: <https://prometheus.org.ua/>,
<http://www.udacity.com>, <https://www.coursera.org>

Зміни та доповнення