

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК



ЗАТВЕРДЖУЮ

Декан факультету КІТ

Інна КОНДІУС

2023 р.



ЗАТВЕРДЖУЮ

Голова НМР

Надія КОВАЛЬЧУК

2023 р.

РОБОЧА ПРОГРАМА

з навчальної дисципліни
**«ТЕХНОЛОГІЇ АДМІНІСТРУВАННЯ ТА ЕКСПЛУАТАЦІЇ
ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»**

ступінь вищої освіти – магістр
галузь знань - 12 «Інформаційні технології»,
спеціальність 122 «Комп'ютерні науки»
ОП Комп'ютерні науки

Форма навчання	Курс	Семестр	Лекції (год.)	Практичні (семінарські, лабораторні) заняття (год.)		Самостійна робота студентів (год.)		Разом (год.)	Залік (сем.)	Екз. (сем.)
				всього лабораторні заняття (год.)	з них тренінг (год.)	всього	з них ІЗ (год.)			
Денна	1	1	15	30	-	105	10	150	1	-
Заочна	1	1	2	6	-	142	10	150	1	-

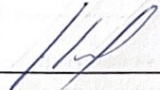
Луцьк – 2023

Робоча програма складена на основі освітньо-професійної програми підготовки магістра галузі знань 12 «Інформаційні технології» спеціальності 122 «Комп'ютерні науки», затвердженої Вченою радою Луцького НТУ (протокол № 10 від 26 05 2022 р.).

Робочу програму склав професор кафедри комп'ютерних наук,
доктор педагогічних наук, кандидат технічних наук,
старший науковий співробітник Ігор КОЗУБЦОВ

Робоча програма затверджена на засіданні кафедри комп'ютерних наук,
протокол № 13 від 08.06. 2023 р.

Завідувач кафедри комп'ютерних наук
кандидат технічних наук,
доцент



Валерій ЛІЩИНА

Розглянуто та схвалено групою забезпечення ОП «Комп'ютерні науки»,
протокол № 4 від 08.06. 2023 р.

Гарант ОП «Комп'ютерні науки»
кандидат технічних наук,
доцент



Валерій ЛІЩИНА

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Технології адміністрування та експлуатації захищених
інформаційно-комунікаційних систем»

1. Опис дисципліни «Технології адміністрування та експлуатації захищених
інформаційно-комунікаційних систем»

Найменування показників	Галузь знань, спеціальність, СВО	Характеристика навчальної дисципліни	
		Денна форма навчання	Заочна форма навчання
Кількість кредитів – 5	галузь знань – 12 «Інформаційні технології»	Статус дисципліни нормативна Мова навчання українська	
Кількість залікових модулів – 3	Спеціальність – 122 «Комп'ютерні науки»	Рік підготовки: 1-й Семестр: 1-й	
Кількість змістових модулів – 2	Ступінь вищої освіти – магістр	Лекції: 15 год. лабораторні заняття: 30 год.	Лекції: 2 год. лабораторні заняття: 6 год.
Загальна кількість годин – 150		Самостійна робота: 105 год. в т. ч. Індивідуальна робота: 10 год.	Самостійна робота: 142 год. в т. ч. Індивідуальна робота: 10 год.
Тижневих годин – 10, з них аудиторних – 3		Вид підсумкового контролю – залік	

2. Мета і завдання дисципліни «Технології адміністрування та експлуатації захищених
інформаційно-комунікаційних систем»

2.1. Мета вивчення дисципліни

Метою викладання навчальної дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем» – є ознайомлення здобувачів вищої освіти з проблемами уразливості інформації в сучасних інформаційно-комунікаційних систем та нормативними документами щодо забезпечення безпеки інформації, існуючими методами та засобами захисту інформації та особливостями їх застосування, нормативно-правовою базою України щодо захисту інформації, принципами впровадження, експлуатації та підтримки захищених інформаційно-комунікаційних систем.

2.2. Завдання вивчення дисципліни

Завданням вивчення навчального курсу «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем» є ознайомлення здобувачів вищої освіти з принципами побудови та використання захищених інформаційних систем; особливостями реалізації систем захисту у інформаційно-комунікаційних системах; закріплення знань щодо принципів адміністрування та експлуатації захищених інформаційно-комунікаційних систем та формування навичок щодо встановлення, налаштування та регулювання роботи програмних засобів захисту інформації.

2.3. Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни

Інтегральна компетентність

Здатність розв'язувати задачі дослідницького та/або інноваційного характеру у сфері комп'ютерних наук.

Загальні компетентності

ЗК01. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК02. Здатність застосовувати знання у практичних ситуаціях.

Фахові компетентності спеціальності

СК05. Здатність розробляти, описувати, аналізувати та оптимізувати архітектурні рішення інформаційних та комп'ютерних систем різного призначення.

СК10. Здатність оцінювати та забезпечувати якість ІТ-проектів, інформаційних та комп'ютерних систем різного призначення, застосовувати міжнародні стандарти оцінки якості програмного забезпечення інформаційних та комп'ютерних систем, моделі оцінки зрілості

процесів розробки інформаційних та комп'ютерних систем.

СК11. Здатність ініціювати, планувати та реалізовувати процеси розробки інформаційних та комп'ютерних систем та програмного забезпечення, включно з його розробкою, аналізом, тестуванням, системною інтеграцією, впровадженням і супроводом.

2.4. Передумови для вивчення дисципліни

Викладання курсу «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем» базуються на знаннях з основ адміністрування комп'ютерних систем та мереж, проектування інформаційних систем, технологій захисту.

2.5. Програмні результати навчання

Після завершення вивчення дисципліни студент повинен:

РН4. Управляти робочими процесами у сфері інформаційних технологій, які є складними, непередбачуваними та потребують нових стратегічних підходів.

РН6. Розробляти концептуальну модель інформаційної або комп'ютерної системи.

РН10. Проектувати архітектурні рішення інформаційних та комп'ютерних систем різного призначення.

РН13. Оцінювати та забезпечувати якість інформаційних та комп'ютерних систем різного призначення.

РН14. Тестувати програмне забезпечення.

РН15. Виявляти потреби потенційних замовників щодо автоматизації обробки інформації.

РН18. Збирати, формалізувати, систематизувати і аналізувати потреби та вимоги до інформаційної або комп'ютерної системи, що розробляється, експлуатується чи супроводжується.

3. Програма навчальної дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем»

Змістовий модуль 1. Забезпечення захисту інформації в захищених інформаційно-комунікаційних системах

Тема 1. Захищені інформаційно-комунікаційні системи

Призначення та класифікація ІКМ та КМ. Структура ІКМ та КМ. Поняття захищеної інформаційно-комунікаційної системи. Проблеми створення захищених інформаційно-комунікаційних систем. Архітектура захищеної мережі.

Література: [1, 2, 3, 4, 6, 8, 9].

Тема 2. Основні загрози безпеці інформації в інформаційно-комунікаційних системах

Види інформації, яка може стати об'єктом злочинних посягань. Класифікації загроз інформаційної безпеки. Типові вразливості систем і аналіз причин їх появи. Класифікація зловмисників. Можливі джерела витоку інформації.

Література: [1, 2, 3, 5, 7, 9, 10, 15].

Тема 3. Система захисту інформації

Основні поняття і визначення. Основні завдання системи захисту інформації. Нормативні документи забезпечення безпеки інформації. Етапи побудови системи безпеки ІС. Методи та засоби забезпечення безпеки інформаційно-комунікаційних систем.

Література: [1, 2, 3, 4, 6, 7, 10, 14, 15].

Змістовий модуль 2. Основи адміністрування та експлуатації захищених інформаційно-комунікаційних систем

Тема 4. Адміністрування інформаційної безпеки

Завдання адміністрування захищених інформаційно-комунікаційних систем. Завдання обліку інформаційної безпеки. Заходи організаційного захисту. Програмне забезпечення для адміністрування ЗІКС та КМ. Протоколювання та аудит.

Література: [1, 2, 3, 4, 14, 15].

Тема 5. Експлуатація і супровід інформаційних систем

Завдання експлуатація захищених інформаційно-комунікаційних систем. Поняття комплексної системи захисту. Основні вимоги до створення комплексної системи захисту.

Створення, введення в дію комплексної системи захисту інформації. Супровід комплексної системи захисту інформації.

Література: [1, 2, 3, 4, 11, 12, 13].

4. Структура залікового кредиту з дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем»

Назви змістових модулів і тем	Кількість годин								Контрольні заходи
	денна форма				заочна форма				
	усього	у тому числі			усього	у тому числі			
		лекції	лабораторні заняття (інші види)	сам.роб. (в т.ч.: ІЗ)		лекції	лабораторні заняття (інші види)	сам.роб. (в т.ч.: ІЗ)	
Змістовий модуль 1. Забезпечення захисту інформації в захищених інформаційно-комунікаційних системах									
Тема 1. Захищені інформаційно-комунікаційні системи	23	1	2	20 (в т.ч.: 2 ІЗ)	23	0,5	1	21,5 (в т.ч.: 2 ІЗ)	МО ₂ , МО ₇ , МО ₉ , МО ₁₀
Тема 2. Основні загрози безпеці інформації в інф.-комунікаційних системах	30	2	8	20 (в т.ч.: 2 ІЗ)	30	0,25	1	28,75 (в т.ч.: 2 ІЗ)	МО ₂ , МО ₇ , МО ₉ , МО ₁₀
Тема 3. Система захисту інформації	28	4	4	20 (в т.ч.: 2 ІЗ)	28	0,25	1	26,75 (в т.ч.: 2 ІЗ)	МО ₂ , МО ₇ , МО ₉ , МО ₁₀
Змістовий модуль 2. Основи адміністрування та експлуатації захищених інформаційно-комунікаційних систем									
Тема 4. Адміністрування інформаційної безпеки	41	4	12	25 (в т.ч.: 2 ІЗ)	41	0,5	2	38,5 (в т.ч.: 2 ІЗ)	МО ₂ , МО ₇ , МО ₉ , МО ₁₀
Тема 5. Експлуатація і супровід інформаційних систем	28	4	4	20 (в т.ч.: 2 ІЗ)	28	0,5	1	26,5 (в т.ч.: 2 ІЗ)	МО ₂ , МО ₇ , МО ₉ , МО ₁₀
Разом	150	15	30	105	150	2	6	142	

5. Теми лабораторних занять

Тема 1. Захищені інформаційно-комунікаційні системи

Лабораторне заняття №1 (2 год. стац. / 1 год. заоч.)

Тема. Архітектура захищеної ІКС.

Мета: Вивчення принципів побудови захищеної ІКС та її зв'язків з КМ.

Завдання для виконання:

1. Визначені індивідуальні завдання згідно методичних вказівок до лабораторних занять з навчальної дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем» №1.

2. Відпрацювання звіту про виконання індивідуального завдання згідно методичних вказівок до лабораторних занять з навчальної дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем».

Література: [1, 2, 3, 4].

Тема 2. Основні загрози безпеці інформації в інформаційно-комунікаційних системах

Лабораторне заняття №2 (4 год. стац. / 0,5 год. заоч.)

Тема. Типові загрози інформаційної безпеки та вразливості ІКС.

Мета: Закріплення знань та вмінь виявлення загроз інформаційної безпеки та вразливості ІКС та аналізу причин їх появи.

Завдання для виконання:

1. Визначені індивідуальні завдання згідно методичних вказівок до лабораторних занять з навчальної дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем» №2.

2. Відпрацювання звіту про виконання індивідуального завдання згідно методичних вказівок

до лабораторних занять з навчальної дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем».

Література: [1, 2, 3, 4].

Лабораторне заняття №3 (4 год. стац. / 0,5 год. заоч.)

Тема. Технічні канали витоку інформації та механізм їх утворення.

Мета: Закріплення знань та вмій виявлення технічних каналів витоку інформації та механізмів їх утворення.

Завдання для виконання:

1. Визначені індивідуальні завдання згідно методичних вказівок до лабораторних занять з навчальної дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем» №3.

2. Відпрацювання звіту про виконання індивідуального завдання згідно методичних вказівок до лабораторних занять з навчальної дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем».

Література: [1, 2, 3, 4].

Тема 3. Система захисту інформації

Лабораторне заняття №4 (4 год. стац. / 1 год. заоч.)

Тема. Методи та засоби забезпечення безпеки інформаційно- комунікаційних систем.

Мета: Систематизація знань та навичок використання методів та засобів захисту інформації в ІКС.

Завдання для виконання:

1. Визначені індивідуальні завдання згідно методичних вказівок до лабораторних занять з навчальної дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем» №4.

2. Відпрацювання звіту про виконання індивідуального завдання згідно методичних вказівок до лабораторних занять з навчальної дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем».

Література: [1, 2, 3, 4].

Тема 4. Адміністрування інформаційної безпеки

Лабораторне заняття №5 (4 год. стац. / 0,5 год. заоч.)

Тема. Організація безпеки ІКС.

Мета: Формування та удосконалення навичок організації безпеки ІКС за допомогою засобів виявлення уразливості локальної мережі.

Завдання для виконання:

1. Визначені індивідуальні завдання згідно методичних вказівок до лабораторних занять з навчальної дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем» №5.

2. Відпрацювання звіту про виконання індивідуального завдання згідно методичних вказівок до лабораторних занять з навчальної дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем».

Література: [1, 2, 3, 4].

Лабораторне заняття №6 (4 год. стац. / 0,5 год. заоч.)

Тема. Організація безпеки даних.

Мета: Формування та удосконалення навичок організації безпеки даних за допомогою засобів виявлення мережних атак.

Завдання для виконання:

1. Визначені індивідуальні завдання згідно методичних вказівок до лабораторних занять з навчальної дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем» №6.

2. Відпрацювання звіту про виконання індивідуального завдання згідно методичних вказівок

до лабораторних занять з навчальної дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем».

Література: [1, 2, 3, 4].

Лабораторне заняття №7 (4 год. стац. / 1 год. заоч.)

Тема. Організація безпеки локальної мережі.

Мета: Формування та удосконалення навичок організації безпеки локальної мережі за допомогою засобів моніторингу трафіку.

Завдання для виконання:

1. Визначені індивідуальні завдання згідно методичних вказівок до лабораторних занять з навчальної дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем» №7.

2. Відпрацювання звіту про виконання індивідуального завдання згідно методичних вказівок до лабораторних занять з навчальної дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем».

Література: [1, 2, 3, 4].

Тема 5. Експлуатація і супровід інформаційних систем

Лабораторне заняття №8 (4 год. стац. / 1 год. заоч.)

Тема. Експлуатація захищених інформаційно-комунікаційних систем.

Мета: Вивчення принципів побудови та введення в дію комплексної системи захисту інформації.

Завдання для виконання:

1. Визначені індивідуальні завдання згідно методичних вказівок до лабораторних занять з навчальної дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем» №8.

2. Відпрацювання звіту про виконання індивідуального завдання згідно методичних вказівок до лабораторних занять з навчальної дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем».

Література: [1, 2, 3, 4].

6. Теми для самостійної роботи

№ п/п	Тематика	К-сть годин	
		денна	заочна
1	Тема 1. Проблеми створення захищених інформаційно-комунікаційних систем. Архітектура захищеної мережі. <i>Література: [1, 2, 3, 4, 6, 8, 9].</i>	18	19,5
2	Тема 2. Класифікації загроз інформаційної безпеки. Типові вразливості систем і аналіз причин їх появи. Класифікація зловмисників. Можливі джерела витоку інформації. <i>Література: [1, 2, 3, 5, 7, 9, 10, 15].</i>	18	26,75
3	Тема 3. Нормативні документи забезпечення безпеки інформації. Етапи побудови системи безпеки ІС. Методи та засоби забезпечення безпеки інформаційно-комунікаційних систем. <i>Література: [1, 2, 3, 4, 6, 7, 10, 14, 15].</i>	18	24,75
4	Тема 4. Заходи організаційного захисту. Програмне забезпечення для адміністрування ЗІКС та КМ. Протоколювання та аудит. <i>Література: [1, 2, 3, 4, 14, 15].</i>	23	36,5
5	Тема 5. Основні вимоги до створення комплексної системи захисту. Створення, введення в дію комплексної системи захисту інформації. Супровід комплексної системи захисту інформації. <i>Література: [1, 2, 3, 4, 11, 12, 13].</i>	18	24,5
	ІЗ	10	10
	Разом	105	142

7. Індивідуальне завдання

Індивідуальне завдання з дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем» виконується самостійно кожним студентом. Підготовка завдання здійснюється на основі опрацьованої літератури та зібраної інформації в мережі Інтернет, її аналізу та формулювання висновків. ІЗ оформляється у відповідності з встановленими вимогами. Метою виконання ІЗ розвиток навичок самостійної роботи, систематизація знань, закріплення теоретичних знань та практичне застосування знань студента з навчального курсу. Виконання ІЗ є одним із обов'язкових складових модулів залікового кредиту з дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем».

Завдання виконання до індивідуального завдання полягає у розв'язанні поставлених завдань (згідно варіанту).

В індивідуальній роботі студенти повинні показати:

- правильне розуміння поставленого завдання;
- вміння працювати з літературними джерелами, використовувати теоретичні знання, отримані на лекціях для розв'язання поставлених завдань;
- здатність розв'язувати спеціалізовані задачі та практичні проблеми під час навчання;
- аргументувати вибір методів розв'язування завдань, обґрунтовувати та захищати прийняті рішення.

8. Методи навчання та оцінювання

Методи навчання:

МН₁ – словесний метод (лекція, дискусія, співбесіда);

МН₂ – практичний метод (лабораторні заняття);

МН₃ – наочний метод (метод ілюстрацій і метод демонстрацій);

МН₄ – робота з навчально-методичною літературою (конспектування, тезування, анотування, рецензування, складання реферату);

МН₅ – відеометод у сполучення з новітніми інформаційними технологіям та комп'ютерними засобами навчання (дистанційні, мультимедійні, веб-орієнтовані, тощо);

МН₆ – самостійна робота;

МН₇ – ІЗ.

Методи оцінювання:

МО₂ – усне опитування;

МО₅ – командні проекти;

МО₇ – презентації результатів виконання завдань та досліджень;

МО₉ – захист лабораторних робіт;

МО₁₀ – залік.

9. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Кожна практична робота, модульне тестування, комплексне практичне індивідуальне завдання оцінюється у 100-бальній системі. Підсумковий бал (за 100-бальною шкалою) з дисципліни «Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем» визначається як середньозважена величина, залежно від вагових коефіцієнтів кожної складової залікового кредиту. Поточний контроль (ПК) – захист усіх лабораторних робіт, (МК) – модульна контрольна робота, ІЗ – виконання індивідуального завдання; МО₁₀ – залік:

Денна форма навчання

Складові залікового кредиту	Заліковий модуль 1		Заліковий модуль 2		Заліковий модуль 3	Разом
	ПК1	МК1	ПК2	МК2	ІЗ	
Ваговий коефіцієнт	20%	25%	20%	25%	10%	100%
	1-8 тиждень	9 тиждень	10-16 тиждень	17 тиждень	18 тиждень	

Шкала оцінювання:

За шкалою ЛНТУ	За національною шкалою	За шкалою ECTS
90–100	зараховано	A (відмінно)
85–89		B (дуже добре)
75-84		C (добре)
65-74		D (задовільно)
60-64		E (достатньо)
35-59	незараховано	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов'язковим повторним курсом)

10. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	Найменування	Номер теми
1.	Мультимедійний проектор, комп'ютер, веб-камера, Інтернет	1-5
2.	Visual Case, VisSim, Arena Rockwell Automation, XJ Technologies Process Charter, Powersim Modell Data AS.	1-5

11. Методичне забезпечення

1. Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем: Конспект лекцій з навчальної дисципліни для здобувачів другого (магістерського) рівня вищої освіти освітньої програми «Комп'ютерні науки» галузі знань 12 Інформаційні технології спеціальності 122 Комп'ютерні науки денної та заочної форм навчання / уклад. І.М. Козубцов. Луцьк: ЛНТУ, 2023. 111 с.

2. Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем: Методичні вказівки до лабораторних занять з навчальної дисципліни для здобувачів другого (магістерського) рівня вищої освіти освітньої програми «Комп'ютерні науки» галузі знань 12 Інформаційні технології спеціальності 122 Комп'ютерні науки денної та заочної форм навчання / уклад. І.М. Козубцов. Луцьк: ЛНТУ, 2022. 49 с.

3. Технології адміністрування та експлуатації захищених інформаційно-комунікаційних систем: Методичні вказівки до самостійної роботи з навчальної дисципліни для здобувачів другого (магістерського) рівня вищої освіти освітньої програми «Комп'ютерні науки» галузі знань 12 Інформаційні технології спеціальності 122 Комп'ютерні науки денної та заочної форм навчання / уклад. І.М. Козубцов. Луцьк: ЛНТУ, 2022. 16 с.

12. Рекомендовані джерела інформації

Базова

4. Технології забезпечення безпеки мережевої інфраструктури / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. К.: КУБГ, 2019. 218 с.

5. Козубцова Л.М., Козубцов І.М., Здолбіцька Н.В., Кошелюк В.А. Показники ефективності функціонування системи захисту інформації і кібербезпеки об'єктів критичної

інформаційної інфраструктури. *Науковий журнал «Комп'ютерно-інтегровані технології: освіта, наука, виробництво»*. 2022. Випуск №48. С. 64 – 69.

6. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.
7. Закон України «Про захист інформації в інформаційно-комунікаційних системах». URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр#Text> (дата звернення: 08.05.2023)
8. Закон України «Про телекомунікації».
9. Концепція технічного захисту інформації в Україні.
10. НД ТЗІ 1.1-002-99: Загальні положення по захисту інформації в комп'ютерних системах від несанкціонованого доступу.
11. НД ТЗІ 3.7-001-99: Методичні вказівки по розробці технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
12. 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.
13. НД ТЗІ 3.7-003-05: Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
14. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою.
15. NIST SP 800-53 Rev. 4 - NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. <https://doi.org/10.6028/NIST.SP.800-53r4>.

Допоміжна

16. Kozubtsov I., Lishchyna N., Kozubtsova L., Trush I., Yashchuk A. Information technology of information security audit of objects of critical infrastructure. *Published on CEUR Workshop Proceedings*. 2022. Vol-3149. Pp. 97–106.
17. Хлапонін Ю.І., Козубцова Л.М., Козубцов І.М., Штонда Р.М. Функції системи захисту інформації і кібербезпеки критичної інформаційної інфраструктури. *Кібербезпека освіта, наука, техніка*. 2022. Том 3. №15. С. 124 – 134. DOI: <https://doi.org/10.28925/2663-4023.2022.15.1241341>
18. Козубцова Л.М., Козубцов І.М., Здолбіцькая Н.В., Кошелюк В.А. Показники ефективності функціонування системи захисту інформації і кібербезпеки об'єктів критичної інформаційної інфраструктури. *Науковий журнал «Комп'ютерно-інтегровані технології: освіта, наука, виробництво»*. 2022. Випуск №48. С. 64 – 69.
19. Козубцов І.М., Козубцова Л.М., Заїчко К.В. Методика розрахунку ефективності функціонування системи захисту інформації й кібербезпеки в інформаційно-комунікаційних системах та оцінювання вкладу окремих показників. *Науково-практичний журнал «Сучасна спеціальна техніка» / Державний науково-дослідний інститут Міністерства внутрішніх справ України*. 2022. №4(71). С. 31 – 44. ISSN 2411-3816.

Інформаційні ресурси

20. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 № 80/94-ВР. <https://zakon.rada.gov.ua/laws/show/80/94-вр#Text>.
21. Закон України «Про інформацію» № 2657-ХП від 02.10.1992. -ВВР, 1992, № 48, ст. 650.
22. Закон України «Про державну таємницю» № 3855-ХП від 21.01.1994, ВВР, 1994, № 16, ст. 93 (остання редакція № 1519-IV від 19.02.2004).
23. Закон України «Про телекомунікації» № 1280-IV, ВВР, 2004, № 12, ст. 155 (остання редакція від 01.02.2007).