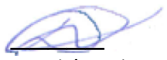
Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)

ЗАТВЕРДЖУЮ

Голова НМК



Д.М.Крицький
(підпис) (ініціали та прізвище)

31.08. 2022 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Кваліфікаційна робота бакалавра
(назва навчальної дисципліни)

Галузь знань: 12 Інформаційні технології
(шифр і найменування галузі знань)

Спеціальність: 123 Комп'ютерна інженерія
(код та найменування спеціальності)

Освітня програма: «Комп'ютерні системи та мережі»
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2022 рік

Розробник: Дужий В.І., доцент кафедри, к.т.н.
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол № 1 від « 30 » 08 2022 р.

Завідувач кафедри д.т.н., професор В. С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td>Найменування показників</td><td>Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td>Характеристика навчальної дисципліни
(денна форма навчання)</td></tr>
<tr><td>Кількість кредитів – 9</td><td rowspan="14">Галузь знань
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність
123 Комп’ютерна інженерія
(код та найменування)

Освітні програми
«Комп’ютерні системи та мережі»

Рівень вищої освіти:

перший (бакалаврський)</td><td>Обов’язкова</td></tr>
<tr><td>Кількість модулів – 1</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістовних модулів – 1</td><td>2022/2023</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання немає</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 270</td><td>8-й</td></tr>
<tr><td>Лекції 1)</td></tr>
<tr><td rowspan="10">Кількість тижневих годин для денної форми навчання:
самостійної роботи студента – 270</td><td>0 годин</td></tr>
<tr><td>Практичні1)</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Лабораторні 1)</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>270 годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>Захист</td></tr>
</table>

2. Мета та завдання навчальної дисципліни

1. Мета: визначення рівня підготовленості студента до розв'язання комплексу учасних наукових і прикладних завдань відповідно до узагальненого об'єкта діяльності на основі застосування системи теоретичних знань і практичних навичок, отриманих у процесі всього періоду навчання відповідно до вимог стандартів вищої освіти.

2. Завдання: систематизація, закріплення і розширення теоретичних знань, отриманих у процесі навчання за освітньо-професійною програмою підготовки фахівця певного освітнього ступеня, і їх практичне використання при вирішенні конкретних наукових, прикладних, інженерних, економіко-соціальних і виробничих питань у певній галузі професійної діяльності; розвиток навичок самостійної роботи, оволодіння методикою досліджень і експериментування, фізичного або математичного моделювання, використання сучасних інформаційних технологій у процесі розв'язання задач, які передбачені завданням на дипломне проектування; визначення відповідності рівня підготовки випускника вимогам освітніх ступенів характеристики фахівця, його готовності та спроможності до самостійної роботи в умовах ринкової економіки, сучасного виробництва, прогресу науки, техніки і культури.

3. Програмні компетентності. Дисципліна має допомогти сформувати у студентів такі компетентності:

ЗК1. Здатність до абстрактного мислення, аналізу і синтезу.

ЗК2. Здатність вчитися і оволодівати сучасними знаннями.

ЗК3. Здатність застосовувати знання у практичних ситуаціях.

ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК5. Здатність спілкуватися іноземною мовою.

ЗК7. Вміння виявляти, ставити та вирішувати проблеми.

ЗК8. Здатність працювати в команді.

ЗК9. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

ЗК10. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя

ФК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп’ютерної інженерії.

ФК2. Здатність використовувати сучасні методи і мови програмування для розроблення алгоритмічного та програмного забезпечення.

ФК3. Здатність створювати системне та прикладне програмне забезпечення комп’ютерних систем та мереж.

ФК4. Здатність забезпечувати захист інформації, що обробляється в комп’ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

ФК5. Здатність використовувати засоби і системи автоматизації проектування до розроблення компонентів комп’ютерних систем та мереж, Інтернет додатків, кіберфізичних систем тощо.

ФК6. Здатність проектувати, впроваджувати та обслуговувати комп’ютерні системи та мережі різного виду та призначення.

ФК7. Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп’ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності.

ФК8. Готовність брати участь у роботах з впровадження комп’ютерних систем та мереж, введення їх до експлуатації на об’єктах різного призначення.

ФК9. Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи.

ФК10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

ФК11. Здатність оформляти отримані робочі результати у вигляді презентацій, науково-технічних звітів.

ФК12. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп’ютерних та кіберфізичних систем, мереж та їхніх компонентів шляхом використання аналітичних методів і методів моделювання.

ФК13. Здатність вирішувати проблеми у галузі комп’ютерних та інформаційних технологій, визначати обмеження цих технологій.

ФК14. Здатність проектувати системи та їхні компоненти з урахуванням усіх аспектів їх життєвого циклу та поставленої задачі, включаючи створення, налаштування, експлуатацію, технічне обслуговування та утилізацію.

ФК15. Здатність аргументувати вибір методів розв’язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати та захищати прийняті рішення.

4. Програмні результати навчання. В результаті вивчення дисципліни студенти мають досягти такі програмні результати навчання:

ПРН4. Знати та розуміти вплив технічних рішень в суспільному, економічному, соціальному і екологічному контексті.

ПРН6. Вміти застосовувати знання для ідентифікації, формулювання і розв’язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.

ПРН11. Вміти здійснювати пошук інформації в різних джерелах для розв’язання задач комп’ютерної інженерії.

ПРН12. Вміти ефективно працювати як індивідуально, так і у складі команди.

ПРН14. Вміти поєднувати теорію і практику, а також приймати рішення та виробляти стратегію діяльності для вирішення завдань спеціальності з урахуванням загальнолюдських цінностей, суспільних, державних та виробничих інтересів.

ПРН16. Вміти оцінювати отримані результати та аргументовано захищати прийняті рішення.

ПРН17. Спілкуватись усно та письмово з професійних питань українською мовою та однією з іноземних мов (англійською, німецькою, італійською, французькою, іспанською).

ПРН19. Здатність адаптуватись до нових ситуацій, обґрунтовувати, приймати та реалізовувати у межах компетенції рішення.

ПРН20. Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення.

ПРН21. Якісно виконувати роботу та досягати поставленої мети з дотриманням вимог професійної етики.

Міждисциплінарні зв'язки: Дисципліна базується на усіх знаннях, отриманих під час вивчення обов'язкових компонентів підготовки у циклі загальної і професійної підготовки, передбачених навчальним планом спеціальності, зокрема:

3. Програма навчальної дисципліни

Модуль 1.
Змістовний модуль 1. Підготовка дипломної роботи та захист
Тема 1. Видача завдання. Постановка задачі.
Тема 2. Аналіз предметної області.
Тема 3. Аналіз існуючих рішень.
Тема 4. Розроблення та/чи аналіз запропонованого рішення.
Тема 5. Нормативно-правове забезпечення
Тема 6. Розроблення пояснювальної записки.
Тема 7. Розроблення презентації та публічний захист.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин *Денна форма*				
	Усього	У тому числі			
		л	п	лаб.	с. р.
1	2	3	4	5	6
Модуль 1					
Змістовний модуль 1. Підготовка дипломної роботи та захист					
Видача завдання. Постановка задачі	2				2
Аналіз предметної області	30				30
Аналіз існуючих рішень	30				30
Розроблення та/чи аналіз запропонованого рішення	40				40
Нормативно-правове забезпечення	20				20
Розроблення пояснювальної записки.	146				146
Розроблення презентації та публічний захист	2				2
Разом за змістовним модулем 1					**270**
Усього годин	**270**				**270**

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	*Не передбачено*	
	Разом	

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання

1	*Не передбачено*	
	Разом	

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	*Не передбачено*	
	Разом	

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	Видача завдання. Постановка задачі	2
2	Аналіз предметної області	30
3	Аналіз існуючих рішень	30
4	Розроблення та/чи аналіз запропонованого рішення.	40
5	Нормативно-правове забезпечення	20
6	Розроблення пояснювальної записки.	146
7	Розроблення презентації та публічний захист	2
	Разом	**270**

9. Індивідуальні завдання

Індивідуальне завдання на дипломну роботу погоджується з дипломним керівником.

10. Методи навчання

Проведення консультацій, а також самостійна робота студентів із використання відповідних матеріалів (п.14, п. 15).

11. Методи контролю

Підсумковий контроль у вигляді публічного захисту.

12. Критерії оцінювання та розподіл балів, які отримують студенти

12.1. Розподіл балів, які отримують студенти (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Самостійна робота	0…65	6	0…65
Публічний захист	0...35	1	0...35
Усього за семестр			**0…100**

12.2. Якісні критерії оцінювання

Дипломна робота має бути виконана у відповідності до закріпленої теми, оформлена згідно затверджених вимог до дипломних робіт і своєчасно представлена до захисту. Автор дипломної роботи повинен продемонструвати: вміння логічно та аргументовано викладати матеріал, коректно використовувати статистичні, математичні та інші методи, проводити власні дослідження; володіння навичками узагальнення, формулювання висновків; вміння працювати з інформаційними джерелами; вміння ініціювати та обґрунтовувати інноваційні підходи до вирішення проблеми, що досліджується.

12.3. Критерії оцінювання роботи студента протягом семестру

Критеріями оцінювання дипломної роботи є:

- чіткість, повнота та послідовність розкриття кожного питання і теми роботи в цілому;
- відсутність орфографічних і синтаксичних помилок;
- правильне оформлення роботи відповідно до стандартів.

Оцінка визначається як сума балів за суть, оформлення і представлення до захисту згідно з наступною орієнтовною шкалою:

1. *Задовільно* (60-74). Показати мінімум знань та умінь. Уміти обґрунтувати тему (актуальність, практичну значимість, сформулювати мету і завдання роботи); продемонструвати результати огляду підходів, аналізу існуючих рішень; продемонструвати результати дослідницької частини (виконання поставлених задач, отримані результати під наглядом керівника,

проєктування, розроблення тощо); уміти працювати над дипломною роботою впродовж семестру під наглядом дипломного керівника.

2. *Добре* (75-89). Твердо знати необхідний обсяг знань для одержання позитивної оцінки, продемонструвати результати огляду підходів, аналізу існуючих рішень, та зроботи постановку задачі; продемонструвати результати дослідницької частини (виконання поставлених задач, самостійно отримані результати, проєктування, розроблення тощо); уміти самостійно та ритмічно працювати над дипломною роботою впродовж семестру.

3. *Відмінно* (90-100). Відмінно знати та демонструвати під час захисту дипломної роботи необхідний обсяг знань для одержання позитивної оцінки. Уміння формулювати напрями подальших досліджень, запропоновувати покращення. Досконально знати всі теми та уміти їх застосовувати. Уміти самостійно та ритмічно працювати над дипломною роботою впродовж семестру.

Розподіл балів, які отримують студенти за виконання дипломної роботи

Пояснювальна записка	Захист роботи	Сума
до 65	до 20	100

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

13. Методичне забезпечення

Навчально-методичний комплекс дісциплини розміщений у системі управління курсами кафедри комп’ютерних систем, мереж та кібербезпеки.

Система управління курсами кафедри комп’ютерних систем, мереж і кібербезпеки [Ел. ресурс]. URL: https://elearn.csn.khai.edu

14. Рекомендована література

Базова

1.Баскаков А. Я. Методология научного исследования : учеб. пособ. для студентов вузов / А. Я. Баскаков, Н. В. Туленков ; Межрегион. Академия упр. Персоналом. – Киев, 2002. – 216с. Шифр: 001 Б27. – Режим доступа: http://library.khai.edu/catalog.

2.Колесников О. В. Основи наукових досліджень : навч. посіб. – 2 -ге вид. випр. та доп. / О. В. Колесников. – Київ : Центр учбової літератури, 2011. – 144 с. – Режим доступу: http://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/OsnjvyMetDoslilKolesnykov2011.pdf

3.Кушнаренко Н. М. Наукова обробка документів : підручник / Н. М. Кушнаренко, В. К. Удалова. – 3-тє вид. – Київ : Знання, 2006. – 332с. Шифр 02 К96. – Режим доступу: http://library.khai.edu/catalog

4. Філіпенко А. С. Основи наукових досліджень : конспект лекцій : посібник: гриф МОН України / А. С. Філіпенко. – Київ : Академвидав, 2004. – 208 с. Шифр: 001 Ф53. – Режим доступу: http://library.khai.edu/catalog

5.Шейко В. М. Організація та методика науково-дослідницької діяльності : підручник : гриф МОН України / В. М. Шейко, Н. М. Кушнаренко. – 5-те вид., стер. – Київ : Знання, 2006. – 307 с. Шифр 001 Ш39. – Режим доступу: http://library.khai.edu/catalog

6.Gorbenko, A., Kharchenko, V., Tarasyuk, O., Furmanov, A.: F(I)MEA-technique of Web Services Analysis and Dependability Ensuring. Lecture Notes in Computer Science, vol. 4157, pp. 153-167 (2006)

7.Babeshko, E., Kharchenko, V., Gorbenko, A.: Applying F(I)MEA-technique for SCADA-based industrial control systems dependability assess- ment and ensuring. In: Third International Conference on Dependability of Computer Systems DEPCOS-RELCOMEX, pp. 309-315 (2008)

8.Bloomfield, R., Netkachova. K., Stroud. R.: Bloomfield, R. Security-Informed Safety: If It's Not Secure, It's Not Safe. In: Software engineering for resilient systems lecture notes in computer science volume 8166, pp. 17-32, Springer Berlin Heidelberg (2013)

9.Ілляшенко, О.О.: Оцінювання інформаційної безпеки систем на програмовній логіці з використанням кейсів: таксономія, нотація, концепція. Наука і Техніка Повітряних Сил Збройних Сил України, № 2(31), с. 97-103 (2018)

10.Illiashenko, O., Potii, O., Komin, D.: Advanced security assurance case based on ISO/IEC 15408. In: Theory and Engineering of Complex Systems зфtand Dependability, Proceedings of the Tenth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX, Advances in Intelligent Systems and Computing, pp. 391-401. Poland, Brunów (2015) (SCOPUS)

11.О. Ілляшенко, Методи і засоби забезпечення виконання вимог до кібербезпеки систем на програмовній логіці: моногр. / за ред. В. С. Харченка. – Міністерство освіти і науки України, Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», 2019. – 195 с.

Допоміжна

1.The Adelard Safety Case Editor – ASCE. In: Adelard. http://www.adelard.co.uk/software/asce/index.html (2010). Accessed 27 Sep 2018

2.Assurance and Safety Case Environment (ASCE) help manual. In: Adelard, Version 4.1. http://www.adelard.com/asce/v4.1/download.html (2010). Accessed 27 Sep 2018

3.Stockham, R.: Emphasis on safety. In: Engineering & Technology Magazine. Vol. 4, Issue 2, pp. 47 – 49 (2009). Accessed 30 Sep 2018

4.Guerra, S., Bishop, P., Bloomfield, R., Sheridan, D.: Assessment and qualification of smart sensors. In: Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies: proceedings of 7th International Topical Meeting 7-11 November 2010. – Las Vegas, pp. 499 – 510 (2010)

5.Nobes, T. S.: Smart instruments in safety instrumented systems. In: InTech, Vol.56, №.7, pp. 14 – 19 (2009)

6.COBRA - security risk analysis & assessment. http://www.riskworld.net/ (2018). Accessed 28 Sep 2018

7.Condor - A system for developing and managing information security policies. Digital Security http://www.dsec.ru/products/kondor/ (2018). Accessed 28 Sep 2018

8.SESAMO. Security and safety modelling. http://sesamo-project.eu. (2018). Accessed 12 Nov 2018

1) **Закони України** .

1. Закон України «Про державну таємницю» від 21 січня 1994, Документ 3855-XII, чинний, поточна редакція — Редакція від 05.08.2018, підстава - 2509-VIII, https://zakon.rada.gov.ua/laws/show/3855-12
2. Закон України «Про інформацію», від 02.10.92, 1992, Документ 2657-XII, чинний, поточна редакція — Редакція від 16.07.2019, підстава - 2704-VIII, https://zakon.rada.gov.ua/laws/main/2657-12
3. Закон України «Про науково-технічну інформацію» від 25.06.1993, Документ 3322-XII, чинний, поточна редакція — Редакція від 19.04.2014, https://zakon.rada.gov.ua/laws/main/3322-12
4. Закон України «Про внесення змін до Закону України "Про захист інформації в автоматизованих системах», Документ 2594-IV, чинний, поточна редакція — Прийняття від 31.05.2005, https://zakon.rada.gov.ua/laws/main/2594-15
5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», 1994, Документ 80/94-ВР, чинний, поточна редакція — Редакція від 19.04.2014, https://zakon.rada.gov.ua/laws/main/80/94-%D0%B2%D1%80
6. Закон України «Про Національну систему конфіденційного зв'язку», 2002, Документ 2919-III, чинний, поточна редакція — Редакція від 19.04.2014, https://zakon.rada.gov.ua/laws/main/2919-14
7. Закон України «Про національну безпеку України» Документ 2469-VIII, чинний, поточна редакція — Прийняття від 21.06.2018, https://zakon.rada.gov.ua/laws/main/2469-19

8. Закон України «Про основні засади забезпечення кібербезпеки України», 2017, Документ 2163-VIII, чинний, поточна редакція — Редакція від 08.07.2018, https://zakon.rada.gov.ua/laws/main/2163-19
9. Указ Президента України «Про заходи щодо захисту інформаційних ресурсів держави» від 10.04.2000, Документ 582/2000, поточна редакція — Прийняття від 10.04.2000, https://zakon.rada.gov.ua/laws/show/582/2000
10. Указ президента україни «Про Положення про технічний захист інформації в Україні», Документ 1229/99, поточна редакція — Редакція від 04.05.2008, https://zakon.rada.gov.ua/laws/show/1229/99
11. Постанова Кабінету Міністрів України від 8 жовтня 1997 р. N 1126 «Про затвердження Концепції технічного захисту інформації в Україні». Документ 1126-97-п, поточна редакція — Редакція від 13.10.2011, підстава - 938-2011-п. https://zakon.rada.gov.ua/laws/main/1126-97-%D0%BF

2) **Укази Президента України.**

1. №1556 от 07.11.2005 "Про додержання прав людини під час проведення оперативно-технічних заходів".
2. № 891 від 24.09.2001 року "Про деякі заходи щодо захисту державних ін формаційних ресурсів у мережах передачі даних".
3. №582 від 10.04 2000 року "Про заходи щодо захисту інформаційних ресурсів держави"
4. № 1229 від 27.09.1999 року "Про Положення про технічний захист ін формації в Україні".
5. № 505 від 22.05. 1998 року "Про Положення про порядок здійснення криптографічного захисту інформації в Україні".

3) **Постанови КМУ**

1. Постанова КМ від 29 березня 2006 р. N 373 " Про затвердження Правил за-безпечення захисту інформації в інформаційних, телекомунікаційних та ін формаційно-телекомунікаційних системах"
2. КМ України Постанова КМ, від 03.08.2005 р. N 688 "Про затвердження Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління"
6. КМ України Постанова КМ, від 28.10.2004 р. N 1452 "Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності"
3. КМ України Постанова КМ, від 28.10.2004 р. N 1453 "Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади"
4. КМ України Постанова КМ, від 28.10.2004 р. N 1454 "Про затвердження Порядку обов'язкової передачі документованої інформації"

5. КМ України Постанова КМ, від 16.11.2002 р. N 1772 "Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах"
6. КМ України Постанова КМ, від 04.02. 1998, N 121 "Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних"
7. КМ України Постанова КМ, від 08.10.1997, № 1126 "Про затвердження Концепції технічного захисту інформації в Україні"
8. КМ України Постанова КМ, від 16.02.1997, №180 "Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах".

4) **Нормативні документи.**

1. НД ТЗІ 2.7-008-08 "Вимоги та рекомендації із забезпечення захисту мовної інформації від витоку акустичним та вібро-акустичним каналами. Методичні вказівки."
2. НД ТЗІ 2.3-017-08 "Методика контролю захищеності мовної інформації від витоку акустичним та вібро-акустичним каналами"
3. НД ТЗІ 2.2-006-08 "Захист інформації на об'єкті інформаційної діяльності. Норми протидії технічній розвідці в акустичному і вібро-акустичному каналах витоку мовної інформації".
4. НД ТЗІ 2.2-003-06 "Протидія технічним розвідкам. Норми з протидії засобам радіолокаційної розвідки"
5. НД ТЗІ 2.3-010-06 "Протидія технічним розвідкам. Методика контролю ефективності протидії засобам радіолокаційної розвідки"
6. НД ТЗІ 2.4-003-06 "Протидія технічним розвідкам. Рекомендації щодо протидії засобам радіолокаційної розвідки"
7. НД ТЗІ 2.3-011-06 "Протидія технічним розвідкам. Методики контролю виконання норм з протидії засобам фотографічної та оптико-електронної розвідок".
8. НД ТЗІ 2.4-004-06 "Протидія технічним розвідкам. Рекомендації з протидії засобам фотографічної та оптико-електронної розвідок".
9. НД ТЗІ 1.6-002-03 "Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації"
10. НД ТЗІ 2.5-010-03 "Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу"
11. 11. НД ТЗІ 2.5-008-2002 "Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2"
12. НД ТЗІ 4.7-002-01 "Визначення захищеності мовної інформації від витоку акустичним і вібро-акустичним каналами. Методичні вказівки"
13. НД ТЗІ 3.6-001-2000 "Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів тех.-нічного захисту інформації від несанкціонованого доступу"

14. НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі"
15. НД ТЗІ Р-001-2000 "Засоби активного захисту мовної інформації з акустичними та вібро-акустичними джерелами випромінювання. Класифікація та загальні технічні вимоги. Рекомендації"
16. НД ТЗІ 1.5-001-2000 "Радіовиявлювачі. Класифікація. Загальні технічні вимоги"
17. НД ТЗІ 2.5-006-99 "Класифікатор засобів копіювально-розмножувальної техніки"
18. НД ТЗІ 2.7-002-99 "Методичні вказівки з використання засобів копіювально-розмножувальної техніки"
19. НД ТЗІ 1.1-001–99 "Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення".
20. НД ТЗІ 2.5-001–99 "Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту"
21. НД ТЗІ 2.5-002-99 "Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту"
22. НД ТЗІ 2.5-003-99 "Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту"
23. НД ТЗІ 2.7-001-99 "Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт"
24. НД ТЗІ 3.7-002-99 "Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова)"
25. НД ТЗІ 1.1-002-99 "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу"
26. НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу"
27. НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу"
28. НД ТЗІ 3.7-001-99 "Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі"

5) **Стандарти**

1. ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96
2. ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96
3. ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ Захист інформації. Технічний захист інформації. Терміни та визначення. ДСТУ 3396.2-97

4. ДЕРЖАВНІ БУДІВЕЛЬНІ НОРМИ УКРАЇНИ Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва ДБН А.2.2-2-96
5. Міжнародні стандарти Режим доступу: https://www.iso.org/ru/home.html
6. Європейські стандарти. Режим доступу: https://www.etsi.org/standards#Security
7. Національні нормативні документи: https://cip.gov.ua/ua/docs
8. ДСТУ EN 61508-1:2019 Функційна безпечність електричних, електронних, програмованих електронних систем, пов'язаних із безпекою. Частина 1. Загальні вимоги (EN 61508-1:2010, IDT; IEC 61508-1:2010, IDT)
9. ДСТУ ISO/IEC 15408-1:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель (ISO/IEC 15408-1:2009, IDT)
10. ДСТУ ISO/IEC 15408-2:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги (ISO/IEC 15408-2:2008, IDT)
11. ДСТУ ISO/IEC 15408-3:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 3. Вимоги до гарантії безпеки (ISO/IEC 15408-3:2008, IDT)
12. ДСТУ ISO/IEC 18045:2015 Інформаційні технології. Методи захисту. Методологія оцінювання безпеки IT (ISO/IEC 18045:2008, IDT)
13. ISO/IEC 15443-1:2012: International Organization for Standardization. International Electrotechnical Commission. Information technology – Security techniques.
14. ISO/IEC TR 15443-2:2012: International Organization for Standardization. International Electrotechnical Commission. Information technology - Security techniques - A framework for IT security assurance – Part 2: Assurance methods.
15. ISO/IEC TR 15443-3:2012: International Organization for Standardization. International Electrotechnical Commission. Information technology - Security techniques - A framework for IT security assurance - Part 3: Analysis of assurance methods.
16. ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT).

15. Інформаційні ресурси

1. Офіційний портал Верховної Ради України [Электрон. ресурс]. – Режим доступа: http://www.rada.gov.ua
2. Законодавство України [Электрон. ресурс]. – Режим доступа: http://zakon3.rada.gov.ua/laws
3. Державна служба спеціального зв'язку та захисту інформації України [Электрон. ресурс]. – Режим доступа: http://dstszi.kmu.gov.ua/dstszi/control/uk/index
4. https://ieeexplore.ieee.org/Xplore/home.jsp
5. https://www.scopus.com/search/form.uri?display=basic
6. https://mjl.clarivate.com/search-results