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 » серпня 2022 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Нормативно -правове забезпечення інформаційної безпеки
(назва навчальної дисципліни)

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

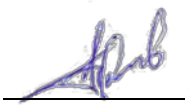
Спеціальність: 125 "Кібербезпека"
(код та найменування спеціальності)

Освітня програма: Безпека інформаційних і комунікаційних систем
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2022 рік

Розробник: Пєвнєв В.Я., доцент кафедри 503, к.т.н., доцент 

(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 – 4</td><td rowspan="10">Галузь знань
1 2 "Інфор мац ійн і технології"
(шифр та найменування)

Спеціальність
125 "Кібербезпека "
(код та найменування)

Освітня програма
Безпека і нформац ійн их і комунікаційних систем
(найменування)

Рівень вищої освіти:
перший (бакалаврський)</td><td>Цикл загальної підготовки</td></tr>
<tr><td>Кількість модулів – 2</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістовних модулів – 3</td><td>2022/2023</td></tr>
<tr><td>Індивідуальне завдання: РР
(назва)</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин: 120</td><td>6-й</td></tr>
<tr><td>Лекції *</td></tr>
<tr><td rowspan="7">Кількість тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи студента – 7,5</td><td>32 годин</td></tr>
<tr><td>Практичні, семінарські*</td></tr>
<tr><td>1 годин</td></tr>
<tr><td>Лабораторні*</td></tr>
<tr><td>32 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>56 годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: 64/56

*Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета: здатність аналізувати сучасні стандарти та формувати загальні вимоги до інформаційної безпеки комп'ютерних систем і мереж.

Завдання: знати систему міжнародних і національних стандартів у галузі кібербезпеки; знати структуру нормативно-правового забезпечення кібербезпеки інформаційно- комунікаційних систем і мереж організацій і підприємств; знати методику оцінювання інформаційної безпеки на відповідність вимогам стандартів. А також:

- навчити студентів використанню нормативних документів ТЗІ, вітчизняних та міжнародних стандартів при розробці систем захисту інформації;
- надати студентам знання з методів сертифікації та оцінки якості технічних та криптографічних засобів захисту інформації;
- ознайомити студентів з базовими міжнародними стандартами в галузі забезпечення інформаційної безпеки.

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

- КЗ 1. Здатність застосовувати знання у практичних ситуаціях.
- КЗ 2. Знання та розуміння предметної області та розуміння професії.
- КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
- КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
- КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.
- КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
- КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
- КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпеки.
- КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
- КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

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

- ПРН 1 застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
- ПРН 2 організовувати власну професійну діяльність, обирати

оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

- ПРН 7 діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;
- ПРН 8 Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.
- ПРН 12 Розробляти моделі загроз та порушника.
- ПРН 16 Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
- ПРН 21 Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
- ПРН 22 Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
- ПРН 23 Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
- ПРН 24 Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
- ПНР 25 Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
- ПРН 26 Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
- ПРН 28 Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
- ПРН 29 Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
- ПРН 37 Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.

- ПРН 38 Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
- ПРН 40 Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації
- ПРН 42 Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
- ПРН 43 Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
- ПРН 44 Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.

Міждисциплінарні зв'язки: Дисципліна є базовою для: «Комплексні системи захисту інформації: проектування, впровадження, супровід», «Кваліфікаційна робота бакалавра».

3. Програма навчальної дисципліни

Модуль 1

Змістовний модуль 1

ТЕМА 1. Правове забезпечення та відповідальність за правопорушення в інформаційній сфері

Вивчається правова основа забезпечення технічного захисту інформації в Україні. Види правових актів, їх визначення. Статті кодексів України відповідно яких наступає відповідальність за правопорушення в інформаційній сфері.

ТЕМА 2. Системи захисту інформації в банківських установах

Розглядаються шляхи забезпечення збереження банківської таємниці. Вимоги щодо захисту інформації у платіжних системах та складові частини системи захисту інформації.

Змістовний модуль №2

ТЕМА 3. Порядок створення, впровадження та супроводження засобів ТЗІ

Вивчається порядок створення, впровадження та супроводження засобів ТЗІ, нормативні документи які регламентують цю діяльність.

ТЕМА 4. Стандарти в сфері криптографічного захисту інформації

Проводиться ознайомлення з міжнародними стандартами в сфері криптографічного захисту інформації та порівняння їх з стандартами України.

ТЕМА 5. Державні стандарти та будівельні норми України. Захист інформації

Ознайомлення та вивчання Державних стандартів та будівельних норми України, які використовуються при розробці комплексів та систем засобів захисту інформаційної структури.

Модульний контроль.

Модуль 2

Змістовний модуль №3

ТЕМА 6. Нормативні документи ТЗІ щодо забезпечення захисту мовної інформації від витоку акустичним та вібро-акустичним каналами

Ознайомлення та вивчання нормативних документів ТЗІ щодо забезпечення захисту мовної інформації від витоку акустичним та вібро-акустичним каналами.

ТЕМА 7. Нормативні документи ТЗІ щодо захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах

Ознайомлення та вивчання нормативних документів ТЗІ щодо захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах.

ТЕМА 8. Нормативні документи ТЗІ щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу

Ознайомлення та вивчання нормативних документів ТЗІ щодо захисту інформації в комп'ютерних системах від несанкціонованого доступ.

Модульний контроль.

4. Структура навчальної дисципліни

Назва змістовного модуля і тем	Кількість годин				
	Усього	У тому числі			
		л	п	лаб.	с. р.
1	2	3	4	5	6
Модуль 1					
Змістовний модуль 1					
Тема 1. Правове забезпечення та відповідальність за правопорушення в інформаційній сфері	23	4		4	15
Тема 2. Системи захисту інформації в банківських установах.	22	4		4	14
Разом за змістовним модулем 2	45	8		8	29
Змістовний модуль 2					
Тема 1. Порядок створення, впровадження та супроводження засобів ТЗІ	16	3		3	10
Тема 2. Стандарти в сфері криптографічного захисту інформації.	18	3		3	12
Тема 3. Державні стандарти та будівельні норми України. Захист інформації.	11	2		2	7
Разом за змістовним модулем 2	45	8		8	29
Усього годин за модуль 1	90	16		16	58
Модуль 2					
Змістовний модуль 3					
Тема 1. Нормативні документи ТЗІ щодо забезпечення захисту мовної інформації від витоку акустичним та вібро-акустичним каналами.	26	6		5	15
Тема 2. Нормативні документи ТЗІ щодо захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах.	26	5		6	15
Тема 3. Нормативні документи ТЗІ щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.	29	5		5	19
РР	9		1		8
Разом за змістовним модулем 3	90	16	1	16	57
Усього годин за модуль 2	90	16	1	16	57
Усього годин за дисципліною	180	32	1	32	115

5. Теми семінарських занять

№ п/п	Назва теми	Кількість годин
	Не передбачено	

6. Теми практичних занять

№ п/п	Назва теми	Кількість годин
1	РР	1
	Разом	**1**

7. Теми лабораторних занять

№ п/п	Назва теми	Кількість годин
1	Дослідження відповідальності за правопорушення в інформаційній сфері	4
2	Дослідження правового забезпечення захисту Інформації в інформаційно-телекомунікаційних системах	4
3	Дослідження об'єктів та видів стандартизації. Сертифікація засобів ТЗІ.	3
4	Дослідження атестації комплексів ТЗІ на об'єктах з різними формами доступу.	3
5	Дослідження державних стандартів ДСТ ЗІ 3396.2-97, ДБН А. 2.2-2-96.	2
6	Дослідження НД ТЗІ-2.2-003-06, 2.3-010-06, 2.3-011-06.	5
7	Дослідження НД ТЗІ 3.7-001-99, 1.4-001-200, 2.5-010-03.	6
8	Дослідження НД ТЗІ 2.2-010-03, 2.5-004-99, 1.1-003-99.	5
	Разом	**32**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Опрацювати: ст. УПК, цивільного кодексу та кодексу про адміністративні порушення в інформаційній сфері.	20
2	Опрацювати: порядок обстеження об'єктів в яких циркулює інформація, що підлягає захисту від несанкціонованого доступу, та оформленням відповідних документів.	20
3	Ознайомитись з міжнародними стандартами в сфері технічного захисту інформації ISO/IEC	25
4	Опрацювати: Нормативні документи ТЗІ щодо забезпечення захисту мовної інформації від витоку акустичним та вібро-акустичним каналами	20
5	Опрацювати: Держстандарти НД ТЗІ2.2-010-03, 2.5-004-99, 1.1-003-99, НД ТЗІ 1.1-002-99, 2.5-004-99, 1.1-003-99	22
6	РР	8
	Разом	**115**

9. Індивідуальні завдання

Розрахункова робота на тему: «Порівняння термінів ЗУ «Про електронні довірчі послуги» та Міжнародних стандартів у сфері ЕЦП ».

10. Теми рефератів

1. Міжнародні стандарти криптографічних методів захисту інформації.
2. Забезпечення захисту інформації в АС.
3. Захист інформації в банківських установах.
4. Захист інформації WEB-сторінки від несанкціонованого доступу.
5. Захист конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах.
6. Правова основа забезпечення технічного захисту інформації в Україні.
7. Комплекси засобів захисту комп'ютерної системи від несанкціонованого доступу.

11. Методи навчання

Проведення аудиторних лекцій, практичних занять, консультацій, а також самостійна робота студентів за відповідними матеріалами (п.14,15).

12. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді іспиту.

10. 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
Модуль 1			
Змістовний модуль 1			
Лекції	0…1	4	0…4
Лабораторні роботи	0...3	2	0…6
Змістовний модуль 2			
Лекції	0…1	4	0…4
Лабораторні роботи	0...3	2	0…6
Модульний контроль	0…25	1	0..25
Модуль 2			
Змістовний модуль 3			
Лекції	0…1	8	0…8

Лабораторні роботи	0…3	4	0…12
Модульний контроль	0…25	1	0…25
РР	0…10	1	0…10
Усього за семестр			**0…100**

12.2. Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки:

- знати ЗУ в галузі технічного захисту інформації;
- знати міжнародні нормативні документи у сфері кібербезпеки;
- знати державні стандарти у сфері кібербезпеки;
- знати НД ТЗІ щодо захисту інформації в мережах та автоматизованих системах.

Необхідний обсяг вмінь для одержання позитивної оцінки:

- використовувати ЗУ для атестації КСЗІ;
- уміти застосовувати національні та міжнародні нормативні документи для вирішення задач побудови системи захисту інформації;
- уміти обґрунтовано вибирати обладнання яке необхідне для побудови КСЗІ і пройшло сертифікацію в державних органах;

12.3. Критерії оцінювання роботи студента протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Захистити не менше 75% від усіх завдань лабораторних занять.

Добре (75-89). Твердо знати мінімум, захистити не менше 90% завдань лабораторних занять.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати.

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

11. Методичне забезпечення

12. Рекомендована література

1. Конституція України
2. Кримінальний кодекс України.
3. Цивільний кодекс України .
4. Кодекс України про адміністративні порушення..

1) Закон України

1. Закон України «Про державну таємницю».

2. Закон України « Про інформацію».
3. Закон України «Про захист інформації в автоматизованих системах».
4. Закон України "Про Державну службу спеціального зв'язку та захисту інформації України".
5. Закон України "Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання" .
6. Закон України "Про ліцензування певних видів господарської діяльності" .
7. Закон України "Про телекомунікації".
8. Закон України "Про електронні документи та електронний документообіг".
9. Закон України "Про електронний цифровий підпис" .
10. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".
11. Закон України "Про основи національної безпеки України".
12. Закон України "Про Національну систему конфіденційного зв'язку".
13. Закон України "Про наукову і науково-технічну експертизу".
14. Закон України "Про ратифікацію Угоди між Кабінетом Міністрів України та Урядом Республіки Білорусь про співробітництво в галузі технічного захисту інформації".
15. Закон України "Про електронні довірчі послуги"

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"
3. 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"
4. КМ України Постанова КМ, від 28.10.2004 р. N 1453 "Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади"
5. КМ України Постанова КМ, від 28.10.2004 р. N 1454 "Про затвердження Порядку обов'язкової передачі документованої інформації"
6. 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"
7. 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"
8. КМ України Постанова КМ, від 08.10.1997, № 1126 "Про затвердження Концепції технічного захисту інформації в Україні"
9. 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 роз-відок".
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. 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

15. Інформаційні ресурси

1. Офіційний портал Верховної Ради України [Электрон. ресурс]. – Режим доступа: http://www.rada.gov.ua
2. . Вікіпедія – вільна енциклопедія [Електрон. ресурс]. Режим доступу: http://www. ru.wikipedia.org/
3. . Вікіпедія - вільна енциклопедія [Електрон. ресурс]. Режим доступу: http://www. ru.wikipedia.org/
4. Wikipedia [Електрон. ресурс]. Режим доступу: http://www. wikipedia.org/
5. . Законодавство України [Електрон. ресурс]. Режим доступу: http://zakon3.rada.gov.ua/laws
6. Державна служба спеціального зв'язку та захисту інформації України [Електрон. ресурс]. - Режим доступу: http://dstszi.kmu.gov.ua/dstszi/control/uk/index