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

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

ЗАТВЕРДЖУЮ

Керівник (гарант) освітньої програми
_____ О.О. Ілляшенко
(підпис) (ініціали та прізвище)

"31" 08 2024 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 2024 рік

Розробник: Піскачов О.І., доцент кафедри 503, к.т.н., снс
(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 2024 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="11">Галузь знань
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність
125 "Кібербезпека"
(код та найменування)

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

Рівень вищої освіти:
перший (бакалаврський)</td><td>Обов’язкова</td></tr>
<tr><td>Кількість модулів – 2</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістових модулів – 3</td><td>2024/2025</td></tr>
<tr><td rowspan="2">Індивідуальне завдання: РР
(назва)</td><td>Семестр</td></tr>
<tr><td>6-й</td></tr>
<tr><td rowspan="2">Загальна кількість годин: 64/120</td><td>Лекції *</td></tr>
<tr><td>32 годин</td></tr>
<tr><td rowspan="6">Кількість тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи студента – 3,5</td><td>Практичні, семінарські*</td></tr>
<tr><td>0 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 colspan="2">Вид контролю</td></tr>
<tr><td colspan="2">Модульний контроль, 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 вивчення: є отримання студентами необхідних знань та навиків для застосування їх з питань механізму правового регулювання відносин, пов'язаних з використанням інформації і захистом останньої від неправомірного використання. А також в подальшому використанню отриманих знань стосовно розробки методів і засобів криптографічного, технічного захисту інформації та при проектування систем захисту інформації. Особлива увага в курсі приділяється вивченню законів, Указів Президента і Постанов Кабінету Міністрів України, нормативних документів технічного захисту інформації, вітчизняних та міжнародних стандартів в галузі захисту та безпеки інформації. Здатність аналізувати сучасні стандарти та сформулювати 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.

Компетентності, які набуваються.

КЗ1. Здатність застосовувати знання у практичних ситуаціях.

КЗ2. Знання та розуміння предметної області та розуміння професії.

КЗ3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

КЗ4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ5. Здатність до пошуку, оброблення та аналізу інформації.

КФ1. 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.

КФ7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

КФ8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

КФ9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпеки.

КФ11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

КФ12. Здатність аналізувати, виявляти та оцінювати можливі загрози, вразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Очікувані результати навчання:

ПРН1 Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

ПРН2 Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

ПРН7 Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

ПРН8 Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

ПРН12 Розробляти моделі загроз та порушника.

ПРН16 Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.

ПРН21 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.

ПРН22 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.

Пререквізити – дисципліна є обов'язковим компонентом освітній програми і базується на знаннях, отриманих під час вивчення дисциплін у циклі загальної і професійної підготовки, передбачених навчальним планом спеціальності.

Кореквізити – «Комплексні системи захисту інформації: проектування, впровадження, супровід», «Кваліфікаційна робота бакалавра».

3. Програма навчальної дисципліни

Модуль 1

Змістовий 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 настає 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.

Змістовий 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 вивчення Державних стандартів та будівельних норм України, які використовуються при розробці комплексів та систем засобів захисту інформаційної структури.

Модульний контроль.

Модуль 2

Змістовий модуль №3

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

Ознайомлення та вивчення нормативних документів ТЗІ щодо забезпечення захисту мовної інформації від витоку акустичним та віброакустичними каналами. Розроблення моделей загроз та порушника.

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

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

Модульний контроль.

4. Структура навчальної дисципліни

Назва змістового модуля і тем	Кількість годин				
	Усього	У тому числі			
		л	п	лаб.	с. р.
1	2	3	4	5	6
Модуль 1					
Змістовий модуль 1					
Тема 1. Правове забезпечення та відповідальність за правопорушення в інформаційній сфері	11	4		4	3
Тема 2. Системи захисту інформації в банківських установах.	11	4		4	3
Разом за змістовим модулем 1	22	8		8	6
Змістовий модуль 2					
Тема 1. Порядок створення, впровадження та супроводження засобів ТЗІ	9	3		3	3
Тема 2. Стандарти в сфері криптографічного захисту інформації.	9	3		3	3
Тема 3. Державні стандарти та будівельні норми України. Захист інформації. Модульний контроль	6	2		2	2
Разом за змістовим модулем 2	24	8		8	8
Усього годин за модуль 1	46	16		16	14
Модуль 2					
Змістовий модуль 3					
Тема 1. Нормативні документи ТЗІ щодо забезпечення захисту мовної інформації від витоку акустичним та віброакустичним каналами.	23	6		5	12
Тема 2. Нормативні документи ТЗІ щодо захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах.	25	5		6	14
Тема 3. Нормативні документи ТЗІ щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Модульний контроль	20	5		5	10
РР	6				6
Разом за змістовим модулем 3	74	16		16	42
Усього годин за модуль 2	74	16		16	42
Усього годин за дисципліною	120	32		32	56

5. Теми семінарських занять

№ п/п	Назва теми	Кількість годин
	Не передбачено	

6. Теми практичних занять

№ п/п	Назва теми	Кількість годин
	Не передбачено	

7. Теми лабораторних занять

№ п/п	Назва теми	Кількість годин
1	Отримання практичних навичок з знаходження відмінностей в визначенні терміну інформації в вітчизняних та закордонних юридичних практиках.	4
2	Отримання практичних навичок з знаходження відмінностей в класифікації персональних даних в вітчизняних та закордонних юридичних практиках.	4
3	Отримання практичних навичок з застосування механізмів сертифікації програмних засобів захисту інформації в Україні.	3
4	Отримання практичних навичок з застосування механізмів сертифікації апаратних засобів захисту інформації в Україні.	3
5	Отримання практичних навичок з застосування міжнародного стандарту ISO 15408	2
6	Отримання практичних навичок з застосування НД ТЗІ 3.7-003 -2005, НД ТЗІ 3.6-007-21	5
7	Отримання практичних навичок з застосування НД ТЗІ 3.7-001-99, НД ТЗІ-1.4-001-2000, НД ТЗІ-2.5-010-03.	6
8	Отримання практичних навичок з застосування НД ТЗІ НД ТЗІ 2.5-008-2002, НД ТЗІ 2.5-004-99, НД ТЗІ 1.1-003-99.	5
	Разом	**32**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Опрацювати: ст. УПК, Цивільного кодексу України та Кодексу про адміністративні порушення в інформаційній сфері.	6
2	Опрацювати: порядок обстеження об’єктів в яких циркулює інформація, що підлягає захисту від несанкціонованого доступу, та оформленням відповідних документів.	8
3	Ознайомитись з міжнародними стандартами в сфері технічного захисту інформації ISO/IEC	12

4	Опрацювати: Нормативні документи ТЗІ щодо забезпечення захисту мовної інформації від витоку акустичним та віброакустичним каналами. Розроблення моделей загроз та порушника	14
5	Опрацювати: НД ТЗІ 2.5-004-99, НД ТЗІ 1.1-002-99, НД ТЗІ-1.1-003-99, НД ТЗІ 3.6-007-21	10
6	РР	6
	Разом	**56**

9. Індивідуальні завдання

Розрахункова робота на тему: «Порівняння термінів Закону України «Про електронну ідентифікацію та електронні довірчі послуги» та міжнародних стандартів у сфері електронного цифрового підпису.

9.1. 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.

10. Методи навчання

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

11. Методи контролю

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

12. Критерії оцінювання та розподіл балів, які отримують здобувачі

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Модуль 1			
Змістовий модуль 1			
Лекції	0…1	4	0…4
Лабораторні роботи	0...3	2	0…6
Змістовий модуль 2			
Лекції	0…1	4	0…4
Лабораторні роботи	0...3	2	0…6
Модульний контроль	0…25	1	0..25
Модуль 2			

Змістовий 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**

Контроль знань при проведенні занять оцінюється за такими шкалами:
активність на лекції під час відповідей на питання:

- повна відповідь на питання - 1 бали;
- неповна відповідь – 0,5 бал;
- відсутність на лекції - 0 балів,

виконання і захист практичних робіт:
при виконанні всіх вимог завдань методик на роботи - 3 бали;

- неповні відповіді на питання при захисті результатів роботи за змістом досліджуваної теми – 2,5 бали;
- неповні відповіді на питання за змістом і результатами роботи - 2 бала;
- недопрацьовані результати роботи і неповні відповіді на питання за змістом результатів роботи -1 бал;
- якщо робота не виконана і не захищена - 0 балів.

На модульний контроль (всього 25 балів) виносяться всі пройдені за контрольований період теми, які включаються в варіанти завдань, що містять по 25 питань (по всім темам та видам занять). Максимальна кількість балів за кожне питання - 1.

Семестровий контроль у вигляді іспиту проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до іспиту. Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Білет для іспиту складається з двох теоретичних та одного практичного запитань, максимальна кількість за кожне із запитань, складає 33 балу.

Критерії оцінювання роботи студента протягом семестру

Задовільно (60-74). Показати достатній мінімум знань та умінь. Захистити не менше 80% від усіх завдань практичних занять. Уміти використовувати правові та нормативні документи, вітчизняні та міжнародні стандарти.

Добре (75-89). Твердо знати необхідний обсяг знань для одержання позитивної оцінки, захистити не менше 90% завдань практичних занять. Уміти використовувати нормативно-правове забезпечення для організації та здійснення заходів з інформаційної безпеки. Мати необхідний обсяг умінь для отримання позитивної оцінки.

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

13. Методичне забезпечення

Навчально-методичний комплекс дисципліни розміщений у системі управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки та у системі дистанційного навчання «Ментор».

Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=3707

14. Рекомендована література

1. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
2. Кримінальний кодекс України. Документ чинний, поточна редакція від 05.10.2023.
URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.
3. Цивільний кодекс України. Документ чинний, поточна редакція від 05.10.2023.
URL: https://zakon.rada.gov.ua/laws/show/435-15#Text.
4. Кодекс України про адміністративні порушення. Документ чинний, поточна редакція від 14.10.2023.
URL:https://zakon.rada.gov.ua/laws/show/80731-10#Text.

Закони України

1. Закон України «Про державну таємницю». Документ, чинний, поточна редакція від 31.03.2023. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text.
2. Закон України « Про інформацію». Документ, чинний, поточна редакція від 27.07.2023.
URL: ttps://zakon.rada.gov.ua/laws/show/2657-12#Text.
3. Закон України «Про захист інформації в автоматизованих системах». Документ, чинний, поточна редакція від 01.07.2022, URL:
https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
4. Закон України "Про Державну службу спеціального зв'язку та захисту інформації України". Документ, чинний, поточна редакція від 31.03.2023.
URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text.
5. Закон України "Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання". Документ чинний, поточна редакція від 17.09.2023.

URL: https://zakon.rada.gov.ua/laws/show/549-15#Text.
6. Закон України "Про електронні документи та електронний документообіг". Документ, чинний, поточна редакція від 01.08.2022. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.
7. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах". Документ , чинний, поточна редакція від 01.07.2022.
URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
8. Закон України "Про Національну систему конфіденційного зв'язку". Документ , чинний, поточна редакція від 01.01.2022.
URL: https://zakon.rada.gov.ua/laws/show/2919-14#Text
9. Закон України "Про наукову і науково-технічну експертизу". Документ , чинний, поточна редакція від 31.03.2023.
URL: https://zakon.rada.gov.ua/laws/show/51/95-%D0%B2%D1%80#Text.
10. Закон України "Про електронну ідентифікацію та електронні довірчі послуги". Документ , чинний, поточна редакція
URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

Укази Президента України.

1. Указ Президента України "Про заходи щодо захисту інформаційних ресурсів держави". Документ 582/2000, поточна редакція від 10.04.2000.
URL: https://zakon.rada.gov.ua/laws/show/582/2000#Text.
2. Указ Президента України "Про Положення про технічний захист інформації в Україні". Документ 1229/99, поточна редакція від 04.05.2008. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text.
3. Указ Президента України "Про Положення про порядок здійснення криптографічного захисту інформації в Україні". Документ, поточна редакція від 12.09.2009. URL: https://zakon.rada.gov.ua/laws/show/505/98#Text.

Постанови КМУ

1. "Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах". Документ, чинний, поточна редакція від 21.10.2022.
URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text.
2. "Про внесення змін до деяких постанов Кабінету Міністрів України щодо електронних комунікацій". Документ, чинний, поточна редакція від 11.04.2023.
URL:https://zakon.rada.gov.ua/laws/show/991-2022-%D0%BF#Text.
3. "Про внесення змін до постанови Кабінету Міністрів України" від 4 лютого 1998 р. Документ, чинний, поточна редакція від 11.11.2009.
URL:https://zakon.rada.gov.ua/laws/show/1191-2009-%D0%BF#Text.
4. "Про затвердження Концепції технічного захисту інформації в Україні. Документ, чинний, поточна редакція від 13.10.2011.
URL:https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF#Text.
9. "Про внесення змін до постанови Кабінету Міністрів України від 16 лютого 1998 р. N 180". Документ, чинний, поточна від 04.08.2010.
URL: https://zakon.rada.gov.ua/laws/show/699-2010-%D0%BF#Text.

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.

15. Інформаційні ресурси

1. Офіційний портал Верховної Ради України [Электрон. ресурс]. Режим доступа: URL: http://www.rada.gov.ua.