


**СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»**

	Ступінь освіти	бакалавр
	Спеціальність	125 Кібербезпека та захист інформації 172 Електронні комунікації та радіотехніка
	Тривалість викладання	9,10 чверті
	Заняття:	Осінній семестр
	лекції:	2 години
	практичні заняття:	1 година
Мова викладання	українська	

Сторінка курсу в СДО НТУ «ДП»:
<https://do.nmu.org.ua/enrol/index.php?id=5403>

Кафедра, що викладає Безпеки інформації та телекомунікацій

Інформація про викладача:



Степанов Михайло Миколайович	професор, с.н.с.
Персональна сторінка	https://bit.nmu.org.ua/ua/pro_kaf/prepods/stepanov.php
E-mail:	stepanov.m.m@nmu.one

1. Анотація до курсу

Студенти навчаються використовувати правничу термінологію у професійній діяльності, аналізувати з позиції нормативно-правового забезпечення інформаційної безпеки складові суспільних відносин, використовувати отримані знання щодо визначення виду юридичної відповідальності за порушення вимог законодавства у сфері інформаційної безпеки; адаптуватися в умовах динамічних змін нормативно-правового забезпечення професійної діяльності, прогнозувати результат та наслідки. Застосовувати диференційний аналіз в роботі з документами, що мають різний правовий статус.

2. Мета та завдання курсу

Мета дисципліни – сформувати необхідну систему знань з основ національного та міжнародного законодавства, яке регулює правові відносини в інформаційній сфері, визначає сутність та зміст механізмів забезпечення інформаційної безпеки, світогляду

щодо сфери забезпечення інформаційної безпеки, різновидів завдань інформаційної безпеки та способів їх вирішення; здобуття теоретичних знань, умінь та навичок.

Завдання курсу полягає у формуванні здатності здобувачів вищої освіти застосовувати законодавчу та нормативно-правову базу забезпечення інформаційної безпеки, а також державні та міжнародні стандарти, вимоги і практики у професійній діяльності в галузі інформаційної та/або кібербезпеки; впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо)..

3. Результати навчання

Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

Володіти та застосовувати в практичній діяльності знання щодо визначення виду юридичної відповідальності за порушення вимог законодавства у сфері інформаційної безпеки.

Адаптуватися в умовах динамічних змін нормативно-правового забезпечення професійної діяльності, прогнозувати результат та наслідки. Застосовувати диференційний аналіз в роботі з документами, що мають різний правовий статус.

4. Структура курсу

ЛЕКЦІЇ

Змістовний модуль №1

1. Основи нормативно-правового забезпечення.

- 1.1 Нормативно-правові акти, які закріплюють концептуальні положення інформаційної безпеки України.
- 1.2 Нормативно-правові акти, які закріплюють визначальні положення щодо забезпечення інформаційної безпеки України.
- 1.3 Нормативно-правові акти, які визначають порядок охорони державної таємниці в Україні.

Змістовний модуль №2

2. Нормативно-правове забезпечення інформаційної та кібернетичної безпеки.

- 2.1 Нормативно-правові акти з інформаційної безпеки комунікаційних систем.
- 2.2 Закони України про електронний документообіг та електронний цифровий підпис.
- 2.3 Підзаконні нормативні акти щодо електронного документообігу та електронного цифрового підпису.
- 2.4 Нормативно-правові акти, які визначають порядок технічного захисту інформації в Україні. Державні та міжнародні стандарти.
- 2.5 Нормативно-правові акти у сфері захисту державних електронних інформаційних ресурсів України.

ПРАКТИЧНІ ЗАНЯТТЯ

1. Дослідження відповідальності за правопорушення в інформаційній сфері.
2. Дослідження правового забезпечення захисту інформації в інформаційно-телекомунікаційних системах.

3. Дослідження об'єктів та видів стандартизації. Сертифікація засобів ТЗІ.

4. Дослідження державних стандартів ДСТ ЗІ 3396.2-97, ДБН А. 2.2-2-96.

5. Технічне обладнання та/або програмне забезпечення

Необхідний доступ до системи дистанційного навчання НТУ «ДП». Активованій акаунт університетської пошти (student.i.p.@nmu.one) на Офіс365.

6. Система оцінювання та вимоги

6.1. Навчальні досягнення здобувачів вищої освіти за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

Рейтингова шкала	Інституційна шкала
90 – 100	відмінно
74 - 89	добре
60 - 73	задовільно
0 - 59	незадовільно

6.2. Здобувачі вищої освіти можуть отримати **підсумкову оцінку** з навчальної дисципліни на підставі поточного оцінювання знань за умови, якщо набрана кількість балів з поточного тестування та самостійної роботи складатиме не менше 60 балів.

Максимальне оцінювання:

Теоретична частина	Практична частина		Бонус	Разом
	При своєчасному складанні	При несвоєчасному складанні		
60	40	28	0	100

Практичні роботи приймаються за контрольними запитаннями до кожної з роботи. Теоретична частина оцінюється за результатами здачі іспиту. Кожний білет містить 2 питання.

6.3. Критерії оцінювання підсумкової роботи

Робота повинна містити розгорнуті відповіді на два питання білету. Якщо робота виконується у дистанційному режимі, то видача номеру білета проходить через систему MS Teams у зазначеній викладачем групі спілкування. В такому режимі виконана робота пишеться вручну, фотографується та відсилається не електронну пошту викладача у впродовж встановленого викладачем часу. За виконану роботу нараховуються бали:

60 балів – дана розгорнута відповідь на два питання;

40 балів – дана розгорнута відповідь на одне питання, але є помилки при розгляді іншого питання, або є несуттєві помилки у відповідях на два питання;

25 балів – дана повна відповідь на одне питання або на два питання зі значними помилками;

15 балів – відповідь на одне питання із значними помилками;

0 балів – відповіді на питання відсутні або повністю невірні, або робота здана несвоєчасно.

7. Політика курсу

7.1. Політика щодо академічної доброчесності

Академічна доброчесність здобувачів вищої освіти є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). Політика щодо академічної доброчесності регламентується положенням "Положення про систему запобігання та виявлення плагіату у Національному технічному університеті "Дніпровська політехніка". <https://cutt.ly/IBesJEc>.

У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

7.2. Комунікаційна політика

Здобувачі вищої освіти повинні мати активовану університетську пошту.

Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту.

7.3. Політика щодо перескладання

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

7.4 Політика щодо оскарження оцінювання

Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку.

7.5. Відвідування занять

Для здобувачів вищої освіти денної форми відвідування занять є обов'язковим. Поважними причинами для неявки на заняття є хвороба, участь в університетських заходах, академічна мобільність, які необхідно підтверджувати документами. Про відсутність на занятті та причини відсутності здобувач вищої освіти має повідомити викладача або особисто, або через старосту.

За об'єктивних причин (наприклад, міжнародна мобільність) навчання може відбуватись в он-лайн формі за погодженням з керівником курсу.

8 Рекомендовані джерела інформації

8.1. Основні

Конституція України - Основний Закон України - Верховна Рада України; Конституція України від 28.06.1996 № 254к/96-ВР чинний, поточна редакція — Редакція від 01.01.2020.

Законодавство України – видавник Верховна Рада України:

1. Цивільний кодекс України від 16.01.2003 №435-IV;
2. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X;
3. Кримінальний кодекс України від 05.04.2001 №2341-III;
4. Закон України «Про державну таємницю» від 21.01.1994 №3855-XII;
5. Закон України «Про національну безпеку України» від 21.06.2018 №2469-VIII;
6. Закон України «Про розвідку» від 17.09.2020 №912-IX;
7. Закон України «Про контррозвідувальну діяльність» від 26.12.2002 №374-IV;
8. Закон України «Про Службу зовнішньої розвідки України» від 01.12.2005 №3160-IV;
9. Закон України «Про Службу безпеки України» від 25.03.1992 №2229-XII;
10. Закон України «Про оборону України» від 06.12.1991 № 1932-XII;
11. Закон України «Про оперативно-розшукову діяльність» від 18.02.1992 №2135-XII;
12. Закон України «Про Державне бюро розслідувань» від 12.11.2015 №794-VIII;
13. Закон України «Про Національну поліцію» від 02.07.2015 №580-VIII;
14. Закон України «Про Бюро економічної безпеки України» від 28.01.2021 №1150-IX;
15. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 №2163-VIII;
16. Закон України «Про інформацію» від 02.10.1992 №2657-XII;
17. Закон України «Про доступ до публічної інформації» від 13.01.2011 №2939-VI;
18. Закон України «Про захист персональних даних» від 01.06.2010 №2297-VI;
19. Закон України «Про науково-технічну інформацію» від 25.06.1993 №3322-XII;
20. Закон України «Про електронні комунікації» від 16.12.2020 №1089-IX;
21. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 №80/94-ВР;
22. Закон України «Про електронні довірчі послуги» від 05.10.2017 №2155-VIII;
23. Закон України «Про електронну комерцію» від 03.09.2015 №675-VIII;
24. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23.02.2006 №3475-IV;
25. Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 №851-IV;
26. Закон України «Про Національну систему конфіденційного зв'язку» від 10.01.2002 №2919-III;
27. Закон України «Про медіа» від 13.12.2022 №2849-IX;
28. Закон України «Про Національну програму інформатизації» від 01.12.2022 №2807-IX;
29. Закон України «Про хмарні послуги» від 17.02.2022 №2075-IX;
30. Закон України «Про цифровий контент та цифрові послуги» від 10.08.2023 №3321-IX;
31. Закон України «Про критичну інфраструктуру» від 16.11.2021 №1882-IX.

Підзаконні нормативно-правові акти - Укази Президента України:

1. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України», Указ Президента України; Стратегія від 14.09.2020 №392/2020;
2. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України», Указ Президента України; Стратегія від 25.03.2021 №121/2021;

3. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України», Указ Президента України; Стратегія від 26.08.2021 №447/2021;
4. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки», Указ Президента України; Стратегія від 28.12.2021 №685/2021;
5. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», Указ Президента України; Доктрина від 25.02.2017 №47/2017;
6. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», Указ Президента України; Стратегія від 15.03.2016 №96/2016;
7. Про Перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць, Президент України; Указ, Перелік від 19.05.2020 №190/2020;
8. Про Положення про порядок підготовки документів щодо надання доступу до державної таємниці іноземцям та особам без громадянства, Президент України; Указ, Положення від 17.07.2006 № 621/2006;
9. Про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, Указ Президента України; Положення від 30.06.2011 №717/2011;
10. Про деякі питання передачі державної таємниці іноземній державі чи міжнародній організації, Президент України; Указ, Положення від 14.12.2004 №1483/2004;
11. Про Положення про порядок здійснення криптографічного захисту інформації в Україні, Указ Президента України від 22.05.1998 №505/98;
12. Про Положення про технічний захист інформації в Україні, Указ Президента України від 27.09.1999 №1229/99;
13. Про рішення Ради національної безпеки і оборони України від 17 червня 1997 року «Про невідкладні заходи щодо впорядкування системи здійснення державної інформаційної політики та удосконалення державного регулювання інформаційних відносин», Президент України; Указ від 21.07.1997 №663/97.

Постанови, розпорядження Кабінету Міністрів України:

14. Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, Постанова Кабінету Міністрів України; Порядок від 16.05.2023 №497;
15. Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього, Постанова Кабінету Міністрів України; Форма типового документа від 28.04.2023 №415;
16. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, Постанова Кабінету Міністрів України; Порядок від 04.04.2023 №299;
17. Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, Постанова Кабінету Міністрів України; Порядок, Звіт, Форма типового документа від 24.03.2023 №257;
18. Деякі питання забезпечення функціонування державних інформаційних ресурсів, Постанова Кабінету Міністрів України; Порядок, Перелік від 30.12.2022 №1500;
19. Про затвердження Положення про державну реєстрацію нормативно-правових актів міністерств та інших органів виконавчої влади, Постанова Кабінету Міністрів України; Положення від 28.12.1992 №731;

20. Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, Кабінет Міністрів України; Постанова, Інструкція від 19.10.2016 №736;
21. Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, Постанова Кабінету Міністрів України від 16.02.1998 №180;
22. Про затвердження Концепції технічного захисту інформації в Україні, Кабінет Міністрів України; Постанова, Концепція від 08.10.1997 №1126;
23. Про затвердження Положення про порядок розроблення, виготовлення, реалізації та придбання спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації, Постанова Кабінету Міністрів України; Положення від 27.10.2001 №1450;
24. Про деякі питання захисту інформації, охорона якої забезпечується державою, Постанова Кабінету Міністрів України; Перелік від 13.03.2002 №281;
25. Про затвердження Порядку надання послуг конфіденційного зв'язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям, Постанова Кабінету Міністрів України; Порядок від 11.10.2002 №1519;
26. Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та електронних комунікаційних системах, Постанова Кабінету Міністрів України; Порядок від 16.11.2002 №1772;
27. Про затвердження Положення про Реєстр інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління, Постанова Кабінету Міністрів України; Положення, Перелік від 03.08.2005 №688;
28. Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, Постанова Кабінету Міністрів України; Правила від 29.03.2006 №373;
29. Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, Постанова Кабінету Міністрів України від 08.02.2021 №92;
30. Деякі питання об'єктів критичної інфраструктури, Постанова Кабінету Міністрів України; Порядок, Перелік, Методика від 09.10.2020 № 1109;
31. Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього, Постанова Кабінету Міністрів України; Форма типового документа, Повідомлення від 28.04.2023 №415;
32. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, Постанова Кабінету Міністрів України; Вимоги, Перелік від 19.06.2019 №518;
33. Про затвердження Технічного регламенту засобів криптографічного захисту інформації, Постанова Кабінету Міністрів України; Технічний регламент від 21.10.2020 №991;
34. Деякі питання організації міжвідомчого обміну інформацією в Національній системі конфіденційного зв'язку, Постанова Кабінету Міністрів України; Положення від 14.05.2015 №303;

35. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, Постанова Кабінету Міністрів України; Порядок від 11.11.2020 №1176;
36. Деякі питання об'єктів критичної інфраструктури, Постанова Кабінету Міністрів України; Порядок, Перелік, Методика від 09.10.2020 №1109;
37. Деякі питання об'єктів критичної інформаційної інфраструктури, Постанова Кабінету Міністрів України; Порядок, Форма типового документа від 09.10.2020 №943;
38. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, Постанова Кабінету Міністрів України; Вимоги, Перелік від 19.06.2019 №518;
39. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку пріоритетних електронних інформаційних ресурсів її суб'єктів, Постанова Кабінету Міністрів України; Положення, Перелік від 14.11.2018 №1024;
40. Про затвердження вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг, Постанова Кабінету Міністрів України; Вимоги, Перелік, Порядок від 07.11.2018 №992;
41. Про реалізацію експериментального проекту щодо запровадження комплексу організаційно-технічних заходів з виявлення вразливостей і недоліків у налаштуванні інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси, Постанова Кабінету Міністрів України; Порядок від 23.12.2020 №1363;
42. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, Постанова Кабінету Міністрів України; Порядок від 23.12.2020 №1295;
43. Деякі питання функціонування Національної телекомунікаційної мережі, Постанова Кабінету Міністрів України; Порядок, Правила від 16.12.2020 №1358;
44. Про затвердження Положення про організаційно-технічну модель кіберзахисту, Постанова Кабінету Міністрів України; Положення від 29.12.2021 №1426;
45. Про схвалення Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації, Розпорядження Кабінету Міністрів України; Стратегія, План, Заходи від 17.11.2021 №1467-р.

Рішення Ради Національної Безпеки і Оборони:

46. Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації, РНБО; Рішення від 29.12.2016 n0015525-16;
47. Про Доктрину інформаційної безпеки України, РНБО; Рішення від 29.12.2016 n0016525-16;
48. Про План реалізації Стратегії кібербезпеки України, РНБО; Рішення, План від 30.12.2021 n0087525-21;
49. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України, РНБО; Рішення від 28.04.2014 n0004525-14.

Правові акти нормативного характеру міністерств, відомств, інших центральних органів виконавчої влади, державних органів – суб'єктів нормотворення:

50. Про затвердження Порядку обробки персональних даних у Національній комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку НКЕК; Постанова, Порядок від 21.12.2022 №261, z0143-23;
51. Про затвердження Зводу відомостей, що становлять державну таємницю, Служба безпеки України; Наказ, Звід від 23.12.2020 №383, z0052-21;
52. Про затвердження Інструкції про порядок забезпечення доступу до публічної інформації у Службі безпеки України, Служба безпеки України; Наказ, Інструкція, Форма, Рекомендації від 14.06.2011 №231, z0851-11;
53. Про затвердження Переліку психічних захворювань (розладів), які можуть завдати шкоди охороні державної таємниці і за наявності яких допуск до державної таємниці громадянину не надається, Спільний наказ МОЗ України, Служба безпеки України; Перелік від 13.05.2002 №174/136, z0458-02;
54. Про затвердження Переліку відомостей, що становлять службову інформацію в Міністерстві внутрішніх справ України, МВС України; Наказ, Перелік від 12.07.2023 №573, v0573320-23;
55. Про затвердження Положення про єдину цифрову відомчу телекомунікаційну мережу МВС, МВС України; Наказ, Положення, Форма типового документа, Умови від 04.07.2016 №596;
56. Про затвердження Переліку відомостей, що становлять службову інформацію в Міністерстві внутрішніх справ України, МВС України; Наказ, Перелік від 12.07.2023 №573, v0573320-23;
57. Про затвердження Переліку відомостей, що становлять службову інформацію у центральному апараті та територіальних управліннях Державного бюро розслідувань, Державне бюро розслідувань; Наказ, Перелік від 29.06.2021 №373, v0373911-21;
58. Про Вимоги з кібербезпеки паливно-енергетичного сектору критичної інфраструктури, Міненерго; Наказ від 15.12.2022 №417;
59. Про затвердження переліків документів нормативно-правової бази, що забезпечує надання відповідного виду послуг у галузі криптографічного та технічного захисту інформації, Адміністрація Держспецзв'язку; Наказ, Перелік від 19.07.2023 №633, v0633519-23;
60. Про затвердження Положення про державну експертизу в сфері криптографічного захисту інформації, Адміністрація Держспецзв'язку; Наказ, Положення, Форма типового документа, Перелік, Рішення, Акт, Висновок від 23.06.2008 №100, z0651-08;
61. Про затвердження Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, Адміністрація Держспецзв'язку; Наказ, Порядок, Повідомлення, Зразок, Форма типового документа від 10.06.2008 №94, 0603-08;
62. Про затвердження Порядку формування й користування інформаційним фондом Реєстру інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління, Адміністрація Держспецзв'язку; Наказ, Порядок, Правила, Форма від 24.04.2007 №72, 0500-07;
63. Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті, Адміністрація Держспецзв'язку; Наказ, Порядок, Акт, Форма типового документа від 15.01.2016 №20;

64. Про затвердження Технічних вимог до основних технічних засобів системи оперативно-технічного управління телекомунікаційними мережами, Адміністрація Держспецзв'язку; Наказ, Вимоги від 14.12.2020 №808;
65. Про затвердження Примірної публічної пропозиції про здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж і Методичних рекомендацій з розроблення публічної пропозиції про здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, Адміністрація Держспецзв'язку; Наказ, Пропозиції, Рекомендації від 14.07.2023 №599;
66. Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами, Адміністрація Держспецзв'язку; Наказ, Рекомендації від 29.05.2023 №463;
67. Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України, Постанова Національного банку України; Положення від 12.08.2022 №178;
68. Про затвердження Положення про захист інформації та кіберзахист учасниками платіжного ринку, Постанова Національного банку України; Положення від 19.05.2021 №43;
69. Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг, Постанова Національного банку України; Положення, Форма типового документа, Звіт від 16.01.2021 №4;
70. Про затвердження Положення про визначення об'єктів критичної інфраструктури в банківській системі України, Постанова Національного банку України; Положення від 30.11.2020 №151;
71. Про затвердження Вимог до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки, Держатомрегулювання; Наказ, Вимоги від 22.03.2022 №223;
72. Про затвердження Переліку відомостей, що становлять службову інформацію в Державному комітеті телебачення і радіомовлення України, Держкомтелерадіо України; Наказ, Перелік від 28.06.2023 №46, v0046603-23.

Міжнародні правові акти:

1. Конвенція про кіберзлочинність, Рада Європи; Конвенція, Міжнародний документ від 23.11.2001 №994_575, Ратифікація від 07.09.2005;
2. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних, Рада Європи; Конвенція, Міжнародний документ від 28.01.1981 №994_326, редакція від 06.07.2010;
3. Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу, Європейський Союз; Директива, Міжнародний документ від 06.07.2016 №2016/1148, 984_013-16.

Нормативні документи системи ТЗІ:

1. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 №806);

2. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 №22;
3. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованих системах, наказ ДСТСЗІ СБУ від 04.12.2000 №53 (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806);
4. НД ТЗІ 1.4-002-2008 Радіолокатори нелінійні. Класифікація. Рекомендовані методи та засоби випробувань, наказ Адміністрації Держспецзв'язку від 14.02.2008 №32;
5. НД ТЗІ 1.5-001-2000 Радіовиявлювачі. Класифікація. Загальні технічні вимоги, наказ ДСТСЗІ СБУ від 13.06.2000 № 29 (Зміна № 1 наказ ДСТСЗІ СБУ від 27.02.2001 №5);
6. НД ТЗІ 1.5-002-2012 Класифікатор засобів технічного захисту інформації, наказ Адміністрації Держспецзв'язку від 29.08.2012 №472;
7. НД ТЗІ 1.6-002-2003 Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації, наказ ДСТСЗІ СБУ від 24.04.2003 №41 (Зміна № 1, наказ Адміністрації Держспецзв'язку від 03.11.2011 №93 дск., зміна № 2, наказ Адміністрації Держспецзв'язку від 17.08.2013 №451);
8. НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці, наказ Адміністрації Держспецзв'язку від 15.04.2013 №215;
9. НД ТЗІ 2.3-001-2001 Радіовиявлювачі вимірювальні. Методи та засоби випробувань, наказ ДСТСЗІ СБУ від 27.02.2001 №5;
10. НД ТЗІ 2.3-002-2001 Технічний захист мовної інформації в симетричних в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань, наказ ДСТСЗІ СБУ від 06.04.2001 №11;
11. НД ТЗІ 2.3-003-2001 Технічний захист мовної інформації в симетричних в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Генератори спеціальних сигналів. Методика випробувань, наказ ДСТСЗІ СБУ від 06.04.2001 №11;
12. НД ТЗІ 2.3-004-2001 Радіовиявлювачі індикаторні. Методи та засоби випробувань, наказ ДСТСЗІ СБУ від 09.04.2001 №12;
13. НД ТЗІ 2.3-006-2001 Радіовиявлювачі аналізу вальні. Методи та засоби випробувань, наказ ДСТСЗІ СБУ від 06.11.2001 №64;
14. Р-001-2000 Засоби активного захисту мовної інформації з акустичними та віброакустичними джерелами випромінювання. Класифікація та загальні технічні вимоги. Рекомендації, наказ ДСТСЗІ СБУ від 04.09.2000 №41;
15. ТР ЕОТ-95 Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоків каналами побічних електромагнітних випромінювань і наводок, наказ Державної служби України з питань ТЗІ від 09.06.95 №25 (Зміна № 1, наказ Адміністрації Держспецзв'язку від 03.11.2011 № 93 дск);
16. ТР ТЗІ – ПЕМВН-95 Тимчасові рекомендації з технічного захисту інформації від витоків каналами побічних електромагнітних випромінювань і наводок, наказ ДСТЗІ від 09.06.95 №25, наказ Державної служби України з питань ТЗІ від 09.06.95 №25, (Зміна № 1, наказ Адміністрації Держспецзв'язку від 03.11.2011 №93 дск);
17. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 №22 (Зміна № 1 наказ від 28.12.2012 №806);

18. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблювальної інформації від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 №22 (Зміна №1 наказ від 15.10.2008 №172);
19. НД ТЗІ 2.5-006-99 Класифікатор засобів копіювально-розмножувальної техніки, наказ ДСТСЗІ СБУ від 26.07.99 №34;
20. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час обробки в автоматизованих системах класу 2, наказ ДСТСЗІ СБУ від 13.12.2002 №84 (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 №806);
21. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB – сторінки від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 02.04.2003 №33 (Зміна №1 наказ від 28.12.2012 №806);
22. НД ТЗІ 2.6-001-2011 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах, наказ Адміністрації Держспецзв'язку від 25.03.2011 №65;
23. НД ТЗІ 2.7-002-99 Методичні вказівки з використання засобів копіювально-розмножувальної техніки, наказ ДСТСЗІ СБУ від 26.07.99 №34;
24. НД ТЗІ 2.7-009-2009 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу, наказ Адміністрації Держспецзв'язку від 24.07.2009 №172 (Зміна №1 наказ від 28.12.2012 №806);
25. НД ТЗІ 2.7-010-2009 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу, наказ Адміністрації Держспецзв'язку від 24.07.2009 №172;
26. НД ТЗІ 2.7-011-2012 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв, наказ Адміністрації Держспецзв'язку від 23.07.2012 №389;
27. 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, наказ ДСТСЗІ СБ України від 20.12.2000 №60 (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 №806);
28. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, наказ ДСТСЗІ СБУ від 28.04.99 №22 (Зміна №1 наказ ДСТСЗІ СБУ від 18.06.2002 №37, зміна №2 наказ Адміністрації Держспецзв'язку від 28.12.2012 №806);
29. НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі, наказ ДСТСЗІ СБ України від 08.11.2005 №125 (Зміна №1 наказ Адміністрації Держспецзв'язку від 28.12.2012 №806);
30. НД ТЗІ 4.7-001-2001 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби визначення наявності та віддаленості місця контактного підключення засобів технічної розвідки. Рекомендації щодо розроблення методів випробувань, наказ ДСТСЗІ СБУ від 06.04.2001 №11;
31. НД ТЗІ 3.6-004-21 Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці;

32. НД ТЗІ 3.6-005-21 Порядок категоріювання безпеки інформаційної системи та інформації;
33. НД ТЗІ 3.6-006-21 Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем;
34. НД ТЗІ 3.6-007-21 Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем;
35. НД ТЗІ 2.3-025-21 Т1 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем);
36. НД ТЗІ 2.3-025-21 Т2 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформацій-них систем;
37. НД ТЗІ 2.3-025-21Т3 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем;
38. НД ТЗІ 2.6-004-21 Порядок авторизації безпеки інформаційних систем;
39. НД ТЗІ 3.6-008-21 Порядок моніторингу безпеки інформаційних систем;
40. ДСТУ 3396.2-97. «Захист інформації. Технічний захист інформації. Терміни та визначення.», 1998;
41. ISO/IEC TR 18044:2004. «Менеджмент інцидентів інформаційної безпеки»;
42. ISO/IEC 27000. «Менеджмент інформаційної безпеки».

8.2. Допоміжні

1. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія / І. В. Арістова, О. А. Баранов, О. П. Дзьобань та ін.; за заг. ред. проф. К. І. Беякова. Київ:КВІЦ, 2019. 344 с. URL: http://ippi.org.ua/sites/default/files/monografiya_ok_0.pdf;
2. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія/О.Д. Довгань, І.М. Доронін; НАПрН України, НДІПІ – К.: Видавничий дім «АртЕк». – 2017. – 107с. URL: http://ippi.org.ua/sites/default/files/eskalaciya_kiberzagroz.pdf ;
3. Правові засади захисту інформації: підручник / Манжай О. В., Манжай І.А. Харків: Панов, 2020. – 162 с. URL: <http://univd.edu.ua/science-issue/issue/4315>;
4. Загальна теорія права: підручник / О. В. Петришин, В. В. Лемак, С. І. Максимов та ін.; Національний юридичний університет ім. Ярослава Мудрого. Харків: Право, 2020. 568 с.
5. Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. – К. : НІСД, 2017. – 496 с.
6. Окінавська хартія глобального інформаційного суспільства від 22.07.2000; URL:<https://ips.ligazakon.net/document/MU00269>

8.3. Інформаційні ресурси

1. Презентації лекцій та практичних занять (електронний варіант).
2. Інтернет-ресурси:
 - <https://zakon.rada.gov.ua>
 - Міжнародні договори, що набули чинності для України та включені до Єдиного державного реєстру нормативно-правових актів (по роках: 1991 – 2023). Сайт Міністерства юстиції України: URL: <https://minjust.gov.ua/> ;

- Зібрання чинних міжнародних договорів України. Сайт Верховної Ради України URL: <https://zakon.rada.gov.ua/laws/main/b94>;
- Зібрання навчальних матеріалів державної освітньої програми «Дія. Цифрова освіта» URL: <https://osvita.diia.gov.ua/>;
- Інформаційне суспільство URL: https://uk.wikipedia.org/wiki/Інформаційне_суспільство ;
- Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, URL: <http://www.nkrzi.gov.ua/index.php?r=site/index&pg=250&language=uk>;
- Нормативно-правове регулювання інформаційних відносин у США URL: <https://www.cisa.gov/>;
- Стратегія кібербезпеки Європейського Союзу URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001>;
- Резолюції ООН, URL: <https://digitallibrary.un.org/record/3951137>;
- Пошукова система у базі лекцій, наукових статей, навчальних посібників та підручників з усього світу/Google Академія - URL: <http://scholar.google.com.ua/>