ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФІЗИЧНИЙ ФАКУЛЬТЕТ
Кафедра твердотільної електроніки та інформаційної безпеки

«ЗАТВЕРДЖУЮ»
Декан фізичного факультету
_____ /Лазур В.Ю./
«__» _____ 2022 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Технології створення й застосування комплексів захисту інформації з обмеженим доступом та охорони об'єктів інформаційної діяльності

Рівень вищої освіти	другий (магістерський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня програма	Системи технічного захисту інформації, автоматизація її обробки
Статус дисципліни	обов’язкова
Мова навчання	українська

Ужгород 2022

Робоча програма навчальної дисципліни «Технології створення та застосування комплексів захисту інформації з обмеженим доступом та охорони об'єктів інформаційної діяльності» для здобувачів вищої освіти галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека освітньо-професійної програми «Системи технічного захисту інформації, автоматизація її обробки».

Розробники: Попович Н. І., доцент, кандидат фіз.-мат. наук, доцент кафедри твердотільної електроніки та інформаційної безпеки ДВНЗ «Ужгородський національний університет»

Робочу програму розглянуто та затверджено на засіданні кафедри

твердотільної електроніки та інформаційної безпеки

протокол № 7 від « 28 » 04 2022 р.

Завідувач кафедри _____ Різак В. М.

Схвалено науково-методичною комісією фізичного факультету

протокол № 10 від « 29 » 04 2022 р.

Голова науково-методичної комісії _____ Карбованець М.І.

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td colspan="2">Розподіл годин за навчальним планом</td></tr>
<tr><td>Денна форма навчання</td><td>Заочна форма навчання</td></tr>
<tr><td>Кількість кредитів ЄКТС – 4</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Загальна кількість годин – 120</td><td>1</td><td></td></tr>
<tr><td>Кількість модулів – 2</td><td colspan="2">Семестр:</td></tr>
<tr><td rowspan="6">Тижневих годин для денної форми навчання:

аудиторних – 3
самостійної роботи студента – 4</td><td>2-ий</td><td></td></tr>
<tr><td colspan="2">Лекції:</td></tr>
<tr><td>18</td><td></td></tr>
<tr><td colspan="2">Практичні (семінарські):</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Лабораторні роботи:</td></tr>
<tr><td>Вид підсумкового контролю: екзамен</td><td>30</td><td></td></tr>
<tr><td colspan="2">Самостійна робота:</td></tr>
<tr><td>Форма підсумкового контролю: усний</td><td>72</td><td></td></tr>
</table>

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення навчальної дисципліни «Технології створення та застосування комплексів захисту інформації з обмеженим доступом та охорони об'єктів інформаційної діяльності» є освоєння технологій створення та ефективного застосування комплексів захисту інформації та охорони об’єктів інформаційної діяльності забезпечення абсолютної захищеності інформації з обмеженим доступом.

Відповідно до освітньої програми, вивчення дисципліни сприяє формуванню у здобувачів вищої освіти таких компетентностей:

ІК. Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного

спрямування; інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.

КФ3. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ6. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ8. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ11. Здатність здійснювати ліцензування, атестацію та сертифікацію засобів та систем захисту інформації на об’єктах інформаційної діяльності

КФ12. Здатність розробляти проектну документацію, програми та методики випробувань, налаштування та супровід комплексів захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури.

3. ПЕРЕДУМОВИ ДЛЯ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Передумовою для вивчення навчальної дисципліни «Технології створення та застосування комплексів захисту інформації з обмеженим доступом та охорони об'єктів інформаційної діяльності» ОПП «Системи технічного захисту інформації, автоматизація її обробки» є навчальна дисципліна «Виявлення та попередження кіберінцидентів».

4. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до ОПП «Системи технічного захисту інформації, автоматизація її обробки», вивчення навчальної дисципліни «Технології створення та застосування комплексів захисту інформації з обмеженим доступом та охорони об'єктів інформаційної діяльності» повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (ПРН):

Програмні результати навчання	Шифр ПРН
Розробляти, застосовувати, інтегрувати, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі у сфері інформаційної безпеки та/або кібербезпеки.	ПРН 4

Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	ПРН 6
Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	ПРН 7
Досліджувати, розробляти і супроводжувати системи та засоби захисту інформації та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	ПРН 8
Досліджувати, розробляти, впроваджувати та використовувати методи та засоби технічного та криптографічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.	ПРН 13
Розробляти, супроводжувати й аналізувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.	ПРН 14
Використовувати методи та засоби виявлення і пошуку закладних пристроїв.	ПРН 26
Аналізувати захищеність території та приміщень об'єкта інформаційної діяльності, технічних засобів і враховувати можливий спектр загроз та їх наслідки для сервісів систем забезпечення інформаційної та кібернетичної безпеки.	ПРН 27

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни «Технології створення та застосування комплексів захисту інформації з обмеженим доступом та охорони об'єктів інформаційної діяльності»:

Очікувані результати навчання	**Шифр ПРН**
Уміння розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі у сфері інформаційної безпеки та/або кібербезпеки.	ПРН 4
Здатність оцінювати захищеність інформаційних систем та комплексів, технологій створення та використання спеціалізованого програмного забезпечення.	ПРН 6
Вміння обгрунтовано впроваджувати та аналізувати кращі світові стандарти, практики для розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	ПРН 7
Навички з розробки та супроводу систем та засобів захисту інформації та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	ПРН 8
Уміння досліджувати, розробляти, впроваджувати та використовувати методи та засоби технічного та криптографічного захисту інформації бізнес/операційних процесів, оцінювати ефективність їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.	ПРН 13

Здатність здійснювати аудит та моніторинг ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки.	ПРН 14
Уміння використовувати методи та засоби виявлення та знешкодження закладних пристроїв.	ПРН 26
Здатність оцінювати захищеність території та приміщень об’єкта інформаційної діяльності, технічних засобів, можливий спектр загроз та їх наслідки для сервісів систем забезпечення інформаційної та кібернетичної безпеки.	ПРН 27

5. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засоби оцінювання та методи демонстрування результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання з навчальної дисципліни «Технології створення та застосування комплексів захисту інформації з обмеженим доступом та охорони об'єктів інформаційної діяльності» є:

- опитування під час захисту лабораторних робіт;
- модульна контрольна робота;
- екзамен.

Форми контролю та критерії оцінювання результатів навчання

Форми поточного контролю: групове або індивідуальне опитування.
Форма модульного контролю: модульна контрольна робота.
Форми підсумкового семестрового контролю: екзамен.

Розподіл балів, які отримують здобувачі вищої освіти (модуль 1)

Поточне оцінювання та самостійна робота				Модульна контрольна робота	Сума
Т1	Т2	Т3	Т4	40	100
15	15	15	15		

Т1-Т4 – теми модуля

Розподіл балів, які отримують здобувачі вищої освіти (модуль 2)

Поточне оцінювання та самостійна робота				Модульна контрольна робота	Сума
Т5	Т6	Т7	Т8	40	100
15	15	15	15		

Т5-Т8 – теми модуля

Оцінювання окремих видів навчальної роботи з дисципліни
«Технології створення та застосування комплексів захисту інформації з обмеженим доступом та охорони об'єктів інформаційної діяльності**»**

Вид діяльності здобувача вищої освіти	**Модуль 1**		**Модуль 2**	
	Кількість	Максимальна кількість балів (сумарна)	Кількість	Максимальна кількість балів (сумарна)
Лабораторні роботи	3	30	4	40
Реферат	1	10	1	10
Модульна контрольна робота	1	60	1	50
Разом		100		100

Критерії оцінювання модульної контрольної роботи

Модульна контрольна робота проводиться у письмовій формі шляхом вирішення тестових завдань. За кожну правильну відповідь тестового завдання студент отримує 2 бали, за неправильну – 0 балів. Перша модульна контрольна робота містить 30 тестових завдань, друга - 25 . Максимальна кількість балів за кожний модуль становить 100 балів

Критерії оцінювання підсумкового семестрового контролю

Підсумковий семестровий контроль з дисципліни **«**Технології створення та застосування комплексів захисту інформації з обмеженим доступом та охорони об'єктів інформаційної діяльності**»»** здійснюється у формі екзамену. Екзамен проводиться за стандартною процедурою. Відповідно до «Положення про порядок та методику проведення семестрових (курсових) екзаменів і заліків в Ужгородському національному університет**і**» (затверджено Наказом Ректора ДВНЗ «УжНУ» No 698/01-17 від 08.05.2015 р.) знання здобувачів оцінюється як з теоретичної, так і з практичної підготовки за такими критеріями:

оцінку «відмінно» (90-100 балів, А) заслуговує здобувач, який: всебічно і глибоко володіє навчально-програмовим матеріалом; вміє самостійно виконувати завдання, передбачені програмою, використовує набуті знання і вміння в нестандартних ситуаціях; засвоїв основну і ознайомлений з додатковою літературою, що рекомендована програмою; засвоїв взаємозв'язок основних понять дисципліни та усвідомлює їх значення для професії, яку він набуває; вільно висловлює власні думки, самостійно оцінює різноманітні ситуації, виявляючи особистісну позицію; самостійно визначає окремі цілі власної навчальної діяльності, виявляє творчі здібності і використовує їх під час вивчення навчально-програмового матеріалу, проявляє нахил до наукової роботи;

оцінку «добре» (82-89 балів, В) заслуговує здобувач, який: повністю опанував і вільно (самостійно) володіє навчально-програмовим матеріалом, у тому числі застосовує його на практиці, має системні знання в достатньому обсязі відповідно до навчально-програмового матеріалу, аргументовано використовує їх у різних

ситуаціях; має здатність до самостійного пошуку інформації, а також до аналізу, постановки і розв'язування проблем професійного спрямування; під час відповіді допустив деякі неточності, які самостійно виправив, добирає переконливі аргументи на підтвердження вивченого матеріалу;

оцінку «добре» (74-81 бал, C) заслуговує здобувач, який: в цілому навчальну програму засвоїв, але відповідає на екзамені з певною кількістю помилок; вміє порівнювати, узагальнювати, систематизувати інформацію під керівництвом викладача, загалом самостійно застосовувати на практиці, контролювати власну діяльність; опанував навчально-програмовий матеріал, успішно виконав завдання, передбачені програмою, засвоїв основну літературу, рекомендовану програмою;

оцінку «задовільно» (64-73 бали, D) заслуговує здобувач, який: знає основний навчально-програмовий матеріал в обсязі, необхідному для подальшого навчання і використання його в майбутній професії; виконує завдання зі значною кількістю помилок; ознайомлений з основною літературою, що рекомендована програмою; допускає на заняттях чи екзамені помилки при виконанні завдань, але під керівництвом викладача знаходить шляхи їх усунення;

оцінку «задовільно» (60-63 бали, E) заслуговує здобувач, який: володіє основним навчально-програмовим матеріалом в обсязі, необхідному для подальшого навчання і використання його у майбутній професії, а виконання завдань задовольняє мінімальні критерії. Знання мають репродуктивний характер.

оцінка «незадовільно» (35-59 балів, FX) виставляється здобувачу, який: виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань;

оцінка «незадовільно» (35 балів, F) виставляється здобувачу, який: володіє навчальним матеріалом тільки на рівні елементарного розпізнавання і відтворення окремих фактів або не володіє зовсім; допускає грубі помилки при виконанні завдань, передбачених програмою; не може продовжувати навчання і не готовий до професійної діяльності після закінчення університету без повторного вивчення даної дисципліни.

При виставленні оцінки враховуються результати навчальної роботи здобувача протягом семестру.

За бажанням студента результуюча підсумкова оцінка може бути визначена як інтегрована оцінка засвоєння всіх тем дисципліни і кількісно дорівнює середньому арифметичному балів, отриманих за кожний модуль. Переведення результатів, отриманих за 100-бальною шкалою оцінювання в національну 4-х бальну та шкалу за системою ECTS здійснюється за наступною схемою:

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Оцінка ECTS</td><td colspan="2">Оцінка за національною шкалою</td></tr>
<tr><td>Екзамен та диференційований залік</td><td>Залік</td></tr>
<tr><td>90 – 100</td><td>A</td><td>відмінно</td><td rowspan="5">Зараховано</td></tr>
<tr><td>82-89</td><td>B</td><td rowspan="2">добре</td></tr>
<tr><td>74-81</td><td>C</td></tr>
<tr><td>64-73</td><td>D</td><td rowspan="2">задовільно</td></tr>
<tr><td>60-63</td><td>E</td></tr>
<tr><td>35-59</td><td>FX</td><td>незадовільно з можливістю повторного складання</td><td>Не зараховано</td></tr>
</table>

0-34	**F**	незадовільно з обов’язковим повторним вивченням дисципліни	

Студент, який отримав за результатами підсумкового контролю отримав оцінку «незадовільно з обов'язковим повторним навчанням» (1-34 балів, F), зобов'язаний пройти повторний курс вивчення дисципліни (під час додаткового семестру) і скласти залік або екзамен. Результати підсумкового контролю знань вносяться до відомості обліку успішності.

6. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

6.1. Зміст навчальної дисципліни

МОДУЛЬ 1. Технології створення комплексів захисту інформації з обмеженим доступом.

Тема 1. Законодавчі та нормативно-правові документи, що визначають створення комплексів захисту інформації на ОІД.

Тема 2. Порядок обстеження об’єкта інформаційної діяльності для виявлення загроз. Вимоги до акту обстеження.

Тема 3. Модель загроз та модель порушника

Тема 4. Технічне завдання на створення комплексу захисту інформації на ОІД. Вибір технічних та криптографічних засобів захисту інформації та охорони ОІД.

МОДУЛЬ 2. Супровід комплексної системи захисту на об’єкті інформаційної діяльності.

Тема 5. Порядок впровадження комплексної системи захисту інформації на об’єкті інформаційної діяльності.

Тема 6. Програмні засоби захисту інформації в КСЗІ.

Тема 7. Оцінювання ефективності функціонування КСЗІ.

Тема 8. Оновлення засобів та технологій КСЗІ у відповідності до зміни умов функціонування ОІД.

6.2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин					
	Форма навчання: денна					
	Усього	у тому числі				
		лекції	практичні (семінарські)	лабораторні	індивідуальна робота	самостійна робота
Змістовий модуль 1 Технології створення комплексів захисту інформації з обмеженим доступом						
1. Законодавчі та нормативно-правові документи, що визначають створення	12	2				10

комплексів захисту інформації на ОІД.						
2. Порядок обстеження об’єкта інформаційної діяльності для виявлення загроз. Вимоги до акту обстеження.	14	2		4		8
3. Розробка моделі загроз та моделі порушника	14	2		4		8
4. Технічне завдання на створення комплексу захисту інформації на ОІД. Вибір технічних та криптографічних засобів захисту інформації та охорони ОІД.	16	2		4		10
Модульна контрольна робота	2			2		
Разом за модуль	58	8		14		36
Змістовий модуль 2. Супровід комплексної системи захисту на об’єкті інформаційної діяльності.						
5. Порядок впровадження комплексної системи захисту інформації на об’єкті інформаційної діяльності.	15	2		4		9
6. Програмні засоби захисту інформації в КСЗІ.	15	2		4		9
Тема 7. Оцінювання ефективності функціонування КСЗІ.	15	2		4		9
8. Оновлення засобів та технологій КСЗІ у відповідності до зміни умов функціонування ОІД.	15	2		4		9
Модульна контрольна робота	2	2				
Разом за модуль	62	10		16		36
Разом всього	**120**	**18**		**30**		**72**

6.3. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		денна	Заочна
1	Обстеження об’єкта інформаційної діяльності	4	
2	Побудова моделі загроз для конкретного ОІД	4	
3	Розробка технічного завдання на створення комплексу захисту інформації на ОІД	4	
4	Впровадження комплексної системи захисту інформації на об’єкті інформаційної діяльності.	4	
5	Впровадження програмних засобів ЗІ	4	
6	Оцінювання ефективності захисту інформації на об’єкті із впровадженою КСЗІ.	4	
7	Дослідження ефективності функціонування КСЗІ на ОІД при зміні умов функціонування.	6	
Разом		**30**	

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин	
		денна	заочна
1	Законодавчі та нормативно-правові акти, що визначають порядок створення та експлуатації систем ТЗІ	10	
2	Етапи розробки КСЗІ	8	
3	Особливості захисту інформаційних систем у воєнний час	8	
4	Особливості захисту інформації та об’єктів критичної інфраструктури під час воєнного стану	10	
5	Особливості проектування та використання системи захисту інформації на ОІД, що здійснюють обробку персональних даних	10	
6	Проведення попередніх випробувань КСЗІ на ОІД, де функціонує інформація з обмеженим доступом	10	
7	Використання інженерних засобів захисту для охорони об’єктів інформаційної діяльності	8	
8	Особливості розробки КЗІ для хмарних інфраструктур	8	
	Разом:	**72**	

7. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

Технічні засоби: технічні засоби навчання (мультимедійний проектор, інтерактивна дошка).
Обладнання: персональні комп’ютер з доступом до мережі Інтернет.
Програмне забезпечення: пакет програм Microsoft Office, додатки Google, платформа для електронного навчання Moodle.

8. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

Основними джерелами інформацію з дисципліни є нормативні документи та рекомендаці, розміщені на сайті можна знайти на сайті Державної служби спеціального зв’язку і захисту інформації:

ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.

НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000 № 53.

НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі

НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Затверджено наказом ДСТСЗІ СБ України від 13.12.2002 № 84.

НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB - сторінки від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 02.04.2003 № 33.

Інформаційні ресурси в мережі Інтернет

1. Сайт Державної служби спеціального зв'язку та захисту інформації України: https://cip.gov.ua/ua/faqs
2. Закон України "Про основні засади забезпечення кібербезпеки України": https://zakon.rada.gov.ua/laws/show/2163-19#Text
3. Постанова Кабінету Міністрів України від 23.12.2020 № 1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки»: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text