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

ТЕООРІЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ З ОБМЕЖЕНИМ ДОСТУПОМ

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 «Теорія захисту інформаційних ресурсів з обмеженим доступом» 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 – 6.5</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Загальна кількість годин – 195</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 – 2 (1-й семестр), 3 (2-й семестр)

самостійної роботи студента – 3 (1-й семестр), 4 (2-й семестр)</td><td>1-ий, 2-ий</td><td></td></tr>
<tr><td colspan="2">Лекції:</td></tr>
<tr><td>36</td><td></td></tr>
<tr><td colspan="2">Практичні (семінарські):</td></tr>
<tr><td>42</td><td></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td rowspan="2">Вид підсумкового контролю: диференційований залік, екзамен</td><td colspan="2">Лабораторні роботи:</td></tr>
<tr><td></td><td></td></tr>
<tr><td rowspan="2">Форма підсумкового контролю: усний</td><td colspan="2">Самостійна робота:</td></tr>
<tr><td>117</td><td></td></tr>
</table>

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення навчальної дисципліни «Теорія захисту інформаційних ресурсів з обмеженим доступом» є засвоєння здобувачами основних понять із захисту інформації, відомостей про математичні моделі захисту інформації, формування у студентів системи теоретичних знань про ймовірні загрози для інформаційного ресурсу, оцінювання ризиків та мінімізації втрат при реалізації загроз для інформації, одержання практичних навичок щодо забезпечення захисту інформації на об'єктах інформаційної діяльності.

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-3. Здатність до абстрактного мислення, аналізу та синтезу.

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.

КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

КФ5. Здатність до дослідження, системного аналізу та забезпечення неперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

3. ПЕРЕДУМОВИ ДЛЯ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

У рамках ОПП «Системи технічного захисту інформації, автоматизація її обробки» другого (магістерського) рівня дисципліна «Теорія захисту інформаційних ресурсів з обмеженим доступом» не потребує передумов для її вивчення.

4. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до ОПП «Системи технічного захисту інформації, автоматизація її обробки», вивчення навчальної дисципліни «Теорія захисту інформаційних ресурсів з обмеженим доступом» повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (ПРН):

Програмні результати навчання	Шифр ПРН
Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі нових результатів досліджень інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.	ПРН 5
Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	ПРН 9
Забезпечувати неперервність бізнес/операційних процесів, виявляти вразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	ПРН 10
Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	ПРН 11
Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати придатні для цього методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.	ПРН 22
Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	ПРН 23
Визначати відомості, які відносяться до інформації з обмеженим доступом, організовувати допуск та доступ персоналу до інформації з обмеженим доступом згідно чинного законодавства та встановленої політики інформаційної та/або кібербезпеки.	ПРН 24

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни «Теорія захисту інформаційних ресурсів з обмеженим доступом»:

Очікувані результати навчання з дисципліни	Шифр ПРН
Вміння критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки на міжгалузевому та міждисциплінарному	ПРН 5

рівні, зокрема на основі нових досягнень інженерних і фізико-математичних наук, використовувати та розвивати технології створення та використання спеціалізованого програмного забезпечення.	
Вміння розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	ПРН 9
Здатність забезпечувати неперервність бізнес/операційних процесів, виявляти вразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	ПРН 10
Уміння аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	ПРН 11
Вміння планувати експериментальні і теоретичні дослідження та виконувати їх, висувати і перевіряти гіпотези, обирати методи та інструменти перевірки гіпотез, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.	ПРН 22
Здатність обгрунтувано вибирати програмне забезпечення, устаткування та інструменти, інженерні технологій і процеси, для забезпечення інформаційної безпеки та/або кібербезпеки, використовуючи знання у суміжних галузях, наукову, технічну та довідкову літературу та іншу доступну інформацію.	ПРН 23
Уміння визначати відомості, які відносяться до інформації з обмеженим доступом, організовувати допуск та доступ персоналу до інформації з обмеженим доступом згідно чинного законодавства та встановленої політики інформаційної та/або кібербезпеки.	ПРН 24

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 «Теорія захисту інформаційних ресурсів з обмеженим доступом» є:

- дискусії на практичних заняттях;
- доповіді та презетації на семінарських заняттях;
- модульна контрольна робота;
- диференційовний залік;
- екзамен.

Форми контролю та критерії оцінювання результатів навчання

Форми поточного контролю: групове або індивідуальне опитування, презентація.
Форма модульного контролю: модульна контрольна робота.

Форми підсумкового семестрового контролю: диференційований залік, екзамен.

Оцінювання окремих видів навчальної роботи з дисципліни «Теорія захисту інформаційних ресурсів з обмеженим доступом»

Вид діяльності здобувача вищої освіти	Модуль 1		Модуль 2	
	Кількість	Максимальна кількість балів (сумарна)	Кількість	Максимальна кількість балів (сумарна)
Практичні (семінарські) заняття	9	18	12	24
Презентація	2	20	2	20
Реферат	1	10	1	10
Модульна контрольна робота	1	52		46
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. Для модуля 1 модульна контрольна робота містить 26 тестових завдань; для модуля 2 - 23 тестових завдання. Максимальна кількість балів за кожний модуль становить 100 балів

Критерії оцінювання підсумкового семестрового контролю

Підсумковий семестровий контроль з дисципліни **«**Теорія захисту інформаційних ресурсів з обмеженим доступом**»** здійснюється у формі диференційованого заліку у першому семестрі та екзамену у другому семестрі. Диференційований залік проводиться в усній формі шляхом співбесіди. 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:

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		Екзамен та диференційований залік	Залік
90 – 100	**A**	Відмінно	Зараховано
82-89	**B**	Добре	
74-81	**C**		
64-73	**D**	задовільно	
60-63	**E**		
35-59	**FX**	незадовільно з можливістю повторного складання	Не зараховано
0-34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	

Студент, який отримав за результатами підсумкового контролю оцінку «незараховано» або «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

Модуль1.

Тема 1. Криза забезпечення безпеки інформації в сучасних умовах. Проблеми теорії захисту інформації.

Тема 2. Основні поняття: інформація та її властивості, захист інформації, інформаційні потоки, ризики, розмежування доступу. Цінність інформації і вартість інформації.

Тема 3. Загрози для інформації. Моделювання поведінки інформаційної системи у випадку реалізації загроз.

Тема 4. Критерії безпеки інформаційних систем. Стандарти інформаційної безпеки. Ефективність захисту інформаційних ресурсів. Міжнародні стандарти інформаційної безпеки, їх еволюція та удосконалення. Універсальність кіберзахисту.

Тема 5. Засоби і методи захисту цілісності інформаційного ресурсу. Доступність інформації. Загрози доступності. Забезпечення доступності інформаційного ресурсу.

Модуль 2.

Тема .6 Поняття загрози інформації. Види загроз. Дестабілізуючі фактори. Модель загроз для середовищ опрацювання інформації. Узагальнений підхід щодо побудови моделі загроз. Аналітичні моделі загроз. Емпіричні моделі загроз.

Тема 7. Поняття політики інформаційної безпеки (ІБ). Основна теорема ІБ. Дискреційна політика безпеки. Мандатна політика безпеки. Рольова політика безпеки. Монітор безпеки. Доказовий підхід.

Тема 8. Загальні моделі інформаційної безпеки. Модель процесу захисту. Модель системи захисту. Модель функцій захисту. Модель з повним перекриттям. Інформаційно-аналітична модель з оцінки захисту інформації від загроз НСД. Модель виявлення порушень. Вартісна модель. Модель взаємодії об'єктів інформаційної системи з точки зору захищеності інформації.

Тема 9. Аналіз безпеки програмного забезпечення. Задача аналізу безпеки ПЗ. Методи аналізу безпеки ПЗ. Нелегітимне використання ресурсів. Нелегітимний доступ до даних. Нелегітимний запуск програм. Нелегітимне виконання програм. Нелегітимна відмова в обслуговування (порушення доступності).

Тема 10. Система управління інформаційною безпекою. Забезпечення неперервності бізнес/операційних процесів. Вразливості інформаційних систем та ресурсів. Аналіз ризиків для інформаційної безпеки.

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
1-й семестр						
Змістовий модуль 1						
Тема 1. Криза забезпечення безпеки інформації в сучасних умовах. Проблеми теорії захисту інформації.	14	2	2			10
Тема 2. Основні поняття: інформація та її властивості, захист інформації, інформаційні потоки, ризики, розмежування доступу. Цінність інформації і вартість інформації.	10	2				8
Тема 3. Загрози для інформації. Моделювання поведінки інформаційної системи у випадку реалізації загроз.	20	4	6			10
Тема 4. Критерії безпеки інформаційних систем. Стандарти інформаційної безпеки. Ефективність захисту інформаційних ресурсів. Міжнародні стандарти інформаційної безпеки, їх еволюція та	22	4	4			14

удосконалення. Універсальність кіберзахисту.						
Тема 5. Засоби і методи захисту цілісності інформаційного ресурсу. Доступність інформації. Загрози доступності. Забезпечення доступності інформаційного ресурсу.	22	4	6			12
Модульна контрольна робота	2	2				
Разом за модуль	90	18	18			54
2-й семестр						
Змістовий модуль 2						
Тема 6. Поняття загрози інформації. Види загроз. Дестабілізуючі фактори. Модель загроз для середовищ опрацювання інформації. Узагальнений підхід щодо побудови моделі загроз. Аналітичні моделі загроз. Емпіричні моделі загроз.	22	4	4			14
Тема 7. Поняття політики інформаційної безпеки (ІБ). Основна теорема ІБ. Дискреційна політика безпеки. Мандатна політика безпеки. Рольова політика безпеки. Монітор безпеки. Доказовий підхід.	26	4	6			16
Тема 8. Загальні моделі інформаційної безпеки. Модель процесу захисту. Модель системи захисту. Модель функцій захисту. Модель з повним перекриттям. Інформаційно-аналітична модель з оцінки захисту інформації від загроз НСД. Модель виявлення порушень. Вартісна модель. Модель взаємодії об'єктів інформаційної системи з точки зору захищеності інформації.	20	4	4			12
Тема 9. Аналіз безпеки програмного забезпечення. Задача аналізу безпеки ПЗ. Методи аналізу безпеки ПЗ. Нелегітимне використання ресурсів. Нелегітимний доступ до даних. Нелегітимний запуск програм. Нелегітимне виконання програм. Нелегітимна відмова в обслуговування (порушення доступності).	18	4	4			10
Тема 10. Система управління інформаційною безпекою. Забезпечення неперервності бізнес/операційних процесів. Вразливості інформаційних систем та ресурсів. Аналіз ризиків для інформаційної безпеки.	17	2	4			11
Модульна контрольна робота	2		2			
Разом за модуль	105	18	24			63
Разом за обидва семестри	**195**	**36**	**42**			**117**

6.3. Теми практичних (семінарських) занять

№ з/п	Назва теми	Кількість годин	
		денна	заочна
1	Властивості інформації з точки зору проблематики її захисту та кібербезпека об'єкту інформаційної діяльності (ОІД)	2	
2	Моделі поведінки інформаційної системи у випадку реалізації загрози для інформації	10	
3	Критерії оцінювання захищеності систем. Стандарти інформаційної безпеки. «Веселкова» серія стандартів інформаційної безпеки.	4	
4	Загрози цілісності та доступності інформаційного ресурсу. Аналіз ризиків.	6	
5	Політика безпеки інформації для зазисту інформаційних ресурсів з обмеженим доступом.	6	
6	Моделювання методів забезпечення безпеки інформаційних ресурсів	4	
7	Захист програмного забезпечення.	4	
8	Забезпечення ефективного управління інформаційною юбезпекою.	4	
Разом		**40**	

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин	
		денна	заочна
1	Інформація з обмеженим доступом: конфіденційна інформація, державна таємниця.	8	
2	Методи і засоби ведення інформаційної війни.	10	
3	Прийоми соціальної інженерії в інформаційних війнах	10	
4	Модель порушника. Мотиви здійснення протиправних дій щодо інформаційного ресурсу	14	
5	Технічна розвідка. Засоби технічної розвідки.	12	
6	Методи контролю цілісності інформації. Організація аудиту інформаційної безпеки.	10	
7	Методи аналізу безпеки програмного забезпечення.	10	
8	Види мережевих атак на електронний інформаційний ресурс.	10	
9	Методи протидії зовнішній кібернетичній агресії	15	
10	Нормативні документи, що стосуються захисту інформаційних ресурсів в умовах воєнного стану	10	
11	Персональні дані як об'єкт хакерських атак. Захист персональних даних.	8	
	Разом:	**117**	

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

1. Закон України «Про основні засади забезпечення **кібербезпеки** України»
2. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020. – 678 с.
3. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. посіб. / В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під. ред. В. М. Богуша. — К.: Видавництво Ліра-К, 2020. — 554 с.
4. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с.

Допоміжна література

1. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту. Монографія / О. Д. Довгань, І. М. Доронін; НАПрН України, НДІІП – К.: Видавничий дім «АртЕк». – 2017. – 107с.

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