Міжнародний гуманітарний університет
Факультет Кібербезпеки, програмної інженерії та комп'ютерних наук
Комп'ютерної інженерії та інноваційних технологій

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Галузь знань 12 Інформаційні технології
Спеціальність 125 « Кібербезпека та захист інформації»
Назва освітньої програми Кібербезпека
Рівень вищої освіти перший (бакалаврський) рівень

Розробники і викладачі	Контактний тел.	E-mail
Доцент кафедри комп'ютерної інженерії та інноваційних технологій **Онацький Олексій Віталійович**	+380503761048	onatsky@meta.ua

1. АНОТАЦІЯ ДО КУРСУ

Дисципліна «Комплексні системи захисту інформації» є обов'язковою складовою освітньо-професійної програми підготовки бакалаврів зі спеціальності 125 «Кібербезпека та захист інформації» та спрямована на формування у здобувачів задач керування по створенню комплексної системи захисту інформації (КСЗІ), аналізувати потреби та вимоги користувачів з метою планування і створення КСЗІ. Дисципліна охоплює основи виникнення загроз витоку, класифікацію технічних каналів (акустичні, електромагнітні, оптичні, віброакустичні), методи та засоби захисту від несанкціонованого доступу до інформації, апаратні комплекси контролю доступу.

Метою викладання дисципліни є забезпечення здобувачів фундаментальними знаннями теоретичних та практичних надбань: з проблем захисту інформацій та інформаційних ресурсів в інформаційно-комунікаційних системах (ІКС) та інформаційно-телекомунікаційних системах (ІТС) від порушення її конфіденційності, цілісності та доступності; основ організації та порядку проведення робіт зі створення КСЗІ; етапів створення КСЗІ; формування вимог до КСЗІ, вимогам щодо захисту інформації від несанкціонованого доступу (НСД); проектування КСЗІ ІКС; введення КСЗІ в ІКС в дію та її супровід.

ПРЕРЕКВІЗИТИ. Передумовами є знання, уміння та навички, отримані при вивченні «Захисту інформації в інфокомунікаційних системах та мережах» (ОК 12), «Криптографії та криптоаналізу» (ОК 23), «Операційних систем» (ОК 20), «Основ Web-безпеки» (ОК 22) та паралельного вивчення «Безпеки програм та даних» (ОК 16).

ПОСТРЕКВІЗИТИ. Знання з проектування та реалізації комплексних систем захисту є безпосередньою базою для вивчення «Управління інформаційною та кібербезпекою» (ОК 30), «Основ цифрової криміналістики» (ОК 26), «Безпеки програм та даних» (ОК 16), «Етичного хакінгу та тестування на проникнення» (ОК 18), а також для проходження переддипломної практики (ОК 35) та підготовки кваліфікаційної роботи (ОК 36).

2. ОЧІКУВАНІ КОМПЕТЕНТНОСТІ, ЯКІ ПЛАНУЄТЬСЯ СФОРМУВАТИ ТА ДОСЯГНЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ

У процесі реалізації програми дисципліни «Комплексні системи захисту інформації» формуються наступні компетентності із передбачених освітньою програмою:

Інтегральна компетентність

ІК. Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі кібербезпеки та захисту інформації.

Загальні компетентності (ЗК)

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності

Спеціальні (фахові, предметні) компетентності

СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).

СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності.

СК 9. Здатність застосовувати методи та засоби технічного захисту інформації на об’єктах інформаційної діяльності.

СК 11. Здатність здійснювати проєктування, адміністрування та керування інформаційно-комунікаційними системами, забезпечуючи їхню надійність, безпеку та ефективність функціонування.

Навчальна дисципліна «Комплексні системи захисту інформації» забезпечує досягнення програмних результатів навчання (РН), передбачених освітньою програмою:

РН 9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації

РН 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

РН 13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.

РН 16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.

РН 17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

РН 20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічною захисту інформації.

РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

РН 22. Вміти застосовувати методи та інструменти проєктування й адміністрування мереж і систем, виконувати налаштування, моніторинг та підтримку їхньої працездатності з урахуванням вимог інформаційної безпеки.

3. ОБСЯГ ТА ОЗНАКИ КУРСУ

Загалом		**Вид заняття** (денне відділення / заочне відділення)				**Ознаки курсу**		
ЄКТС	**годин**	**Лекційні заняття**	**Лабораторні заняття**	**Практичні заняття**	**Самостійна робота**	**Курс, (рік навчання)**	**Семестр**	**Обов'язкова / вибіркова**
5	150	26/6	20/4	14/2	90/138	3	6	**Обов'язкова**

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	**Кількість годин**									
	Денна форма					**Заочна форма**				
	усього	**у тому числі**				**усього**	**у тому числі**			
		лекц.	**лаб.**	**прак.**	**сам. роб.**		**лекц.**	**лаб.**	**прак.**	**сам. роб.**
Тема 1. Нормативно-правове забезпечення захисту інформації.	18	2	2	2	12	20	2			18
Тема 2. Етапи створення КСЗІ. Порядок проведення робіт із створення КСЗІ в ІКС. Формування вимог до КСЗІ.	20	4	2	2	12	22			2	20
Тема 3. Обґрунтування необхідності створення КСЗІ. Категоріювання ІКС.	24	4	4	2	14	22		2		20
Тема 4. Обстеження середовищ функціонування ІКС. Опис моделі порушника політики безпеки інформації. Опис моделі загроз для інформації.	20	4	2	2	12	22	2			20
Тема 5. Формування завдання на створення КСЗІ. Розробка політики безпеки інформації в ІКС.	22	4	2	2	14	22		2		20

Тема 6. Розробка технічного завдання на створення КСЗІ. Розробка проекту КСЗІ.	22	4	4	2	12	20				20
Тема 7. Введення КСЗІ в дію та оцінка захищеності інформації в ІКС. Супровід КСЗІ.	24	4	4	2	14	22	2			20
Усього годин	**150**	**26**	**20**	**14**	**90**	**150**	**6**	**4**	**2**	**138**
ПІДСУМКОВИЙ КОНТРОЛЬ – ЕКЗАМЕН										

5. ТЕХНІЧНЕ Й ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ / ОБЛАДНАННЯ

Студенти отримують теми та питання курсу, основну і додаткову літературу, рекомендації, завдання та оцінки за їх виконання як традиційним шляхом, так і з використанням університетської платформи он-лайн навчання на базі Moodle. Окрім того, практичні навички у пошуку та аналізу інформації за курсом, з оформлення індивідуальних завдань, тощо, студенти отримують, користуючись університетськими комп'ютерними класами та бібліотекою.

6. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «Комплексні системи захисту інформації» включаються:

1. Знайомство з науковою та навчальною літературою відповідно зазначених у програмі тем.
2. Опрацювання лекційного матеріалу.
3. Підготовка до практичних занять.
4. Консультації з викладачем протягом семестру.
5. Самостійне опрацювання окремих питань навчальної дисципліни.
6. Підготовка та виконання індивідуальних завдань у вигляді есе, рефератів тощо.
7. Підготовка до підсумкового контролю.

Тематика та питання до самостійної підготовки та індивідуальних завдань

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	Тема 1. Системний підхід до побудови комплексних систем захисту інформації. Поняття комплексної системи захисту інформації (КСЗІ) як об'єкта проєктування. Принципи побудови КСЗІ (комплексність, безперервність, своєчасність). Життєвий цикл КСЗІ. Взаємозв'язок організаційних, технічних та програмних заходів.	12	18
2	Тема 2. Нормативно-правове регулювання та категоріювання об'єктів. Законодавча база України у сфері КСЗІ. Порядок категоріювання об'єктів інформаційної діяльності (НД ТЗІ 1.6-005-2013). Вимоги до захисту інформації залежно від категорії об'єкта. Державна експертиза КСЗІ.	12	20
3	Тема 3. Моделювання загроз та оцінка ризиків у КСЗІ. Розробка моделі загроз для об'єкта інформаційної діяльності. Методики кількісної та якісної оцінки ризиків. Визначення актуальних загроз та вразливостей. Обґрунтування необхідності створення КСЗІ.	14	20
4	Тема 4. Політика безпеки та організаційні заходи захисту. Розробка політики інформаційної безпеки організації.	12	20

	Організаційна структура служби захисту інформації. Режимні заходи та робота з персоналом. Інструкції та регламенти з безпеки. Обстеження середовищ функціонування ІКС, моделі порушника, моделі загроз.		
5	Тема 5. Проєктування КСЗІ: технічне завдання та обґрунтування. Порядок розробки технічного завдання на створення КСЗІ (НД ТЗІ 1.6-005-2013). Вибір засобів захисту та їх обґрунтування. Профіль захисту та функціональні вимоги безпеки. Етапи проєктування системи.	14	20
6	Тема 6. Впровадження, введення в дію та атестація КСЗІ. Порядок проведення робіт із створення КСЗІ (НД ТЗІ 3.7-003-2023). Процедури введення системи в промислову експлуатацію. Атестація робочих місць та системи в цілому. Оформлення експлуатаційної документації.	12	20
7	Тема 7. Експлуатація, аудит та оцінка ефективності КСЗІ. Організація супроводу КСЗІ. Моніторинг інформаційних процесів та реагування на інциденти. Методи оцінки ефективності функціонування КСЗІ. Проведення аудиту безпеки та інтерпретація результатів.	14	20
	Всього	**90**	**138**

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю	**Складові оцінювання**	
	Для екзамену	**Для заліку**
поточний контроль, який здійснюється у ході: проведення практичних (лабораторних) занять, виконання самостійної роботи, індивідуальних завдань, дослідна робота здобувача тощо.	**50%**	**100%**
підсумковий контроль	**50%**	

Методи діагностики знань (контролю)	фронтальне опитування; наукова доповідь, реферати, усне повідомлення, індивідуальне опитування; робота у групах; ділова гра, розв`язання ситуаційних завдань, кейсів, практичних завдань, залік, екзамен

8. ОЦІНЮВАННЯ ЗДОБУВАЧІВ ВИЩОЇ ТА ФАХОВОЇ ПЕРДВИЩОЇ ОСВІТИ ЗА НАВЧАЛЬНУ ДИСЦИПЛІНУ У МІЖНАРОДНОМУ ГУМАНІТАРНОМУ УНІВЕРСИТЕТІ

(*поточний контроль, підсумковий контроль, загальний результат оцінювання)*

ЕКЗАМЕН

Поточний контроль			
Види роботи	**Планові терміни виконання**	**Форми контролю та звітності**	**Максимальний відсоток оцінювання**
Систематичність і активність роботи на практичних (лабораторних) заняттях			
1.1. Підготовка до практичних (лабораторних) занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних (лабораторних) занять	**30**
Виконання завдань для самостійного опрацювання			
1.2. Індивідуальне тестування, завдання, підготовка реферату (есе) за заданою тематикою	Відповідно до робочої програми та розкладу занять	Розгляд відповідного матеріалу під час аудиторних занять або ІКР[1], перевірка конспектів навчальних текстів тощо	**10**
Виконання індивідуальних завдань, дослідна робота здобувача			
1.3. Інші види індивідуальних завдань, в т.ч. підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	Відповідно до робочої програми та розкладу занять	Обговорення результатів проведеної роботи під час аудиторних занять, наукових конференцій та круглих столів.	**10**
Разом балів за поточний контроль			**50**
Підсумковий контроль екзамен			**50**
Загальний результат оцінювання			**100**

Поточний контроль знань здобувачів освіти при формі контролю **екзамен** (максимум 50 балів) оцінюється за шкалою *(«2», «3», «4», «5»)*, з обов'язковим переведенням балів за кожний вид роботи таким чином:

- за підготовку до аудиторних занять (максимум 30 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості практичних (лабораторних) занять, для переводу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 6;

[1] Індивідуально-консультативна робота викладача зі здобувачами

- за виконання завдань для самостійного опрацювання (тестування, завдання, підготовка реферату (есе) за заданою тематикою) (максимум 10 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості програмного матеріалу, що виноситься на самостійне вивчення, для переводу зазначених балів середньоарифметична оцінка множиться на коефіцієнт 2;
- за інші види індивідуальних завдань, в т.ч. підготовку наукових публікацій, участь у роботі круглих столів, конференцій тощо (максимум 10- балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості інших видів індивідуальних завдань, для переводу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 2.

КРИТЕРІЇ ОЦІНЮВАННЯ ЗА ПОТОЧНИЙ КОНТРОЛЬ

- «2»- виставляється за неправильну відповідь (письмову роботу), яка не відповідає змісту теми та свідчить про нерозуміння її основних положень;
- «3» -виставляється за відповідь (письмову роботу), яка відповідає змісту теми, але є неповною і неточною у визначенні понять, свідчить про неповне розуміння основних положень навчального матеріалу, свідчить про те, що знання студента мають фрагментарний, поверховий характер;
- «4» - оцінюється правильна і обґрунтована відповідь (письмова робота), з якої видно, що студент знає й розуміє теоретичний матеріал в обсязі навчальної теми, володіє необхідними навичками, не допускає суттєвих помилок.
- «5» - оцінюється повна, правильна, ґрунтовна відповідь (письмова робота) на запитання теми, що передбачає логічність і послідовність викладу матеріалу, володіння термінологією, показує вміння повно й глибоко використовувати теоретичні знання в практичній площині.

КРИТЕРІЇ ОЦІНЮВАННЯ ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ ЗДОБУВАЧІВ ЗА ІСПИТ
(максимум 50 балів)

Рівень знань оцінюється:

- від 40 до 50 балів - студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки;
- 30 до 40 балів - студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді;
- 20 - 30 балів - студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки.
- 10 - 20 балів - володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих;
- 0 10 балів - володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки.

9. КРИТЕРІЇ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ
(для екзамену / заліку)

Рівень знань оцінюється:

- «відмінно» / «зараховано» А - від 90 до 100 балів. Студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та семінарських заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної

роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;

- «добре» / «зараховано» B - від 82 до 89 балів. Студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях та семінарських заняттях, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» C - від 74 до 81 балів. Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, реферату та активність у науково-дослідній роботі;
- «задовільно» / «зараховано» D - від 64 до 73 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, рефератів (есе);
- «задовільно» / «зараховано» E - від 60 до 63 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки, має неповний конспект з завданнями до самостійної роботи.
- «незадовільно з можливістю повторного складання» / «не зараховано» FX – від 35 до 59 балів. Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.
- «незадовільно з обов'язковим повторним вивченням дисципліни» / «не зараховано» F – від 0 до 34 балів. Студент не володіє навчальним матеріалом.

ТАБЛИЦЯ ВІДПОВІДНОСТІ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗА РІЗНИМИ ШКАЛАМИ

<table>
<tr><th rowspan="2">100-бальною шкалою</th><th rowspan="2">Шкала за ECTS</th><th colspan="2">За національною шкалою</th></tr>
<tr><th>екзамен</th><th>залік</th></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 rowspan="2">Незадовільно</td><td rowspan="2">Не зараховано</td></tr>
<tr><td>1-34</td><td>F</td></tr>
</table>

10. ДОТРИМАННЯ ВИМОГ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

Викладання та засвоєння навчальної дисципліни передбачає неухильне дотримання вимог академічної доброчесності, яка регулюється Законом України "Про освіту" (Відомості Верховної Ради (ВВР), 2014, № 37-38, ст.2004), «Методичними рекомендаціями для закладів вищої освіти з підтримки принципів академічної доброчесності» (Лист МОН № 1/9-650 від 23.10.18 року), іншими нормативними документами. Зокрема, основні засади дотримання академічної доброчесності визначено у «Положенні про академічну доброчесність у Міжнародному гуманітарному університеті», «Кодексі академічної доброчесності Міжнародного гуманітарного університету» та «Інструкції щодо процедури технічної перевірки на наявність текстових запозичень (академічного плагіату)», затвердженої наказом МГУ від 03.05.2024 р., № 708а.

Відповідно до ст.42 Закону України "Про освіту" академічна доброчесність - це сукупність етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

Дотримання академічної доброчесності передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);
- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Про внесення змін до Закону України "Про інформацію" № 2938-VI від 13.01.2011. – Відомості Верховної Ради України 2011, № 32, ст. 313.
2. Закон України "Про захист персональних даних" № 2297-VI від 01.06.2010. – Відомості Верховної Ради України 2010, № 34, ст. 481.
3. Закон України "Про критичну інфраструктуру" № 2684-IX від 18.10.2022.
4. Онацький О.В., Йона Л.Г., Бєлова Ю.В. Криптографічний захист інформації: Навч. посібник. - Одеса: Одеса : «Астропринт» 2023. 252с. https://surl.li/onvhbl
5. Йона Л.Г., Онацький О.В., Швець О.В. Системи банківської безпеки: Навч. посібник.- Одеса: ДУІТЗ. 2022. 192с. https://surl.lt/hpdpub
6. Онацький О. В., Йона Л. Г. Криптографічні системи : навчальний посібник з дисциплін "Криптографія та криптоаналіз" для освітньо-професійної підготовки бакалаврів в галузі знань 12 "Інформаційні технології" за спеціальністю 125 "Кібербезпека" / О. В. Онацький, Л. Г. Йона. – Одеса : Міжнародний гуманітарний університет, 2023. – 156 с. https://surl.li/oqiqhk
7. НД ТЗІ 3.7-003-2023 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі (Наказ Адміністрації Держспецзв'язку від 28.10.2023 № 924).
8. НД ТЗІ 2.5-004. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – Затверджено наказом ДСТСЗІ СБ України № 22.
9. НД ТЗІ 2.5-005. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – Затверджено наказом ДСТСЗІ СБ України № 22.

10. Положення про Державну експертизу в сфері технічного захисту інформації. – Затверджено наказом Адміністрації ДССЗЗІ України № 93 від 16.05.07.

11. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. – Затверджено наказом Адміністрації ДССЗЗІ України № 65 від 12 березня 2011.

12. 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.

13. НД ТЗІ 2.3-025-21 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, затверджений наказом Адміністрації Держспецзв'язку від 01.02.2022 року № 53.

14. НД ТЗІ 3.6-005-21 Порядок категоріювання безпеки інформаційної системи та інформації.

15. НД ТЗІ 2.6-004-21 Порядок авторизації безпеки інформаційних систем.

16. НД ТЗІ 3.6-008-21 Порядок моніторингу безпеки інформаційних систем.

Допоміжна

17. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.

18. ДСТУ 3396.1. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

19. 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.

20. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

21. Про внесення змін до Закону України "Про захист інформації в автоматизованих системах" № 2594-IV від 31.05.2005. – Відомості Верховної Ради України 2005, № 26, ст. 347.

22. Домарєв В.В., Скворцов С.О. Організація захисту інформації на об'єктах державної та підприємницької діяльності. Навчальний посібник. – К.: Вид-во Європ. Ун-ту, 2006. – 102 с.

23. Онацький О.В. Методологія створення комплексної системі захисту інформацій / 68-ма науково-технічна конференція професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів. Частина ІІІ. Одеса 4-6 груд. – 2013.– С. 152-155.

24. Онацький О.В. Аналіз стандартів інформаційної безпеки. Матеріали 71-ої науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів ОНАЗ ім. О.С. Попова. Частина І. Одеса 6-8 грудня. – 2016. – С. 71 – 74.

25. Онацький О.В. Аналіз програмних і технічних засобів захисту інформації. Матеріали 72-га науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів ОНАЗ ім. О.С. Попова. Частина І. Одеса 13-15 грудня. – 2017. – С. 135 – 137.

26. Онацький О.В. Аналіз системи виявлення вторгнень. Матеріали 72-га науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів ОНАЗ ім. О.С. Попова. Частина І. Одеса 13-15 грудня. – 2017. – С. 106 – 107.

27. Онацький О.В. Створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Матеріали 72-га науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів ОНАЗ ім. О.С. Попова. Частина І. Одеса 13-15 грудня. – 2017. – С. 152 – 154.

28. Онацький О.В. Щодо питань захисту інформаційних ресурсів медичних підприємств. Матеріали 75-а науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів ОНАЗ ім. О.С. Попова. Частина І. Одеса 11-15 грудня. – 2020. – С. 122 – 124.

29. Онацький О.В. Аналіз комплексів засобів захисту від несанкціонованого доступу на базі операційної системи. 73-я науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів ОНАЗ ім. О.С. Попова 12-14 грудня 2018 р. – С. 145 – 146.

30. Онацький О.В. Аналіз та розробка методики управління інцидентами у сфері інформаційної безпеки підприємства. 76-й Науково-технічній конференції професорсько-викладацького складу, науковців, аспірантів та студентів**.** Одеса 15-16 грудня. – 2021 р.

Інформаційні ресурси

31. Сайт Державної служби спеціального зв'язку та захисту інформації. URL: https://cip.gov.ua/ua

32. Сайт Технічний захист інформації. URL: https://tzi.ua/ua/index.html

33. Комплексні системи захисту інформації. URL: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/

34. Комплексні системи захисту інформації. Проектування, впровадження, супровід. URL: https://books.google.com.ua/books?id=GcBlDwAAQBAJ&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

35. Сайт Computer Emergency Response Team of Ukraine. URL: https://cert.gov.ua

36. https://zakon.rada.gov.ua/laws