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

«ЗАТВЕРДЖУЮ»
Декан фізичного факультету
_____ /Лазур В.Ю./
«29» 04 2022 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Ліцензування, атестація та сертифікація у сфері безпеки 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 «Ліцензування, атестація та сертифікація у сфері безпеки 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 – 4.5</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Загальна кількість годин – 135</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 – 5</td><td>1-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></td><td></td></tr>
<tr><td colspan="2">Лабораторні роботи:</td></tr>
<tr><td>Вид підсумкового контролю: екзамен</td><td>18</td><td></td></tr>
<tr><td>Форма підсумкового контролю: усний</td><td colspan="2">Самостійна робота:</td></tr>
<tr><td></td><td>81</td><td></td></tr>
</table>

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення навчальної дисципліни «Ліцензування, атестація та сертифікація у сфері безпеки об'єктів інформаційної діяльності» є освоєння порядку ліцензування, атестації та сертифікації систем, засобів і пристроїв для захисту об’єктів 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-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

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.

КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій,

бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

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

У рамках ОПП «Системи технічного захисту інформації, автоматизація її обробки» другого (магістерського) рівня дисципліна «Ліцензування, атестація та сертифікація у сфері безпеки об'єктів інформаційної діяльності» не потребує передумов для її вивчення.

4. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до ОПП «Системи технічного захисту інформації, автоматизація її обробки», вивчення навчальної дисципліни «Ліцензування, атестація та сертифікація у сфері безпеки об'єктів інформаційної діяльності» повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (ПРН):

Програмні результати навчання	**Шифр ПРН**
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
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
Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних й непередбачуваних ситуаціях, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень	ПРН 16
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
Здійснювати оцінювання захищеності інформації, яка циркулює на об’єкті інформаційної діяльності; аналізувати стан безпеки комп’ютерних систем та мереж.	ПРН 25
Використовувати методи та засоби виявлення і пошуку закладних пристроїв.	ПРН 26
Аналізувати захищеність території та приміщень об’єкта інформаційної діяльності, технічних засобів і враховувати	ПРН 27

можливий спектр загроз та їх наслідки для сервісів систем забезпечення інформаційної та кібернетичної безпеки.	

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни ««Ліцензування, атестація та сертифікація у сфері безпеки об'єктів інформаційної діяльності»:

Очікувані результати навчання з дисципліни	**Шифр ПРН**
Набути навичок використання кращих світових стандартів і практик для розв’язання складних задач професійної діяльності у сфері захисту інформації.	ПРН 7
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
Уміти приймати рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних й непередбачуваних ситуаціях із застосуванням методів та засобів оптимізації, прогнозування та прийняття рішень	ПРН 16
Уміти 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
Вміти оцінювати захищеність інформації, яка циркулює на об’єкті інформаційної діяльності; аналізувати стан безпеки комп’ютерних систем та мереж.	ПРН 25
Уміти користуватися методами та засобами виявлення і пошуку закладних пристроїв.	ПРН 26
Уміти оцінювати 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.	ПРН27

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 «Ліцензування, атестація та сертифікація у сфері безпеки 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, зазист лабораторних робіт.

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
«Ліцензування, атестація та сертифікація у сфері безпеки 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	3	30
Реферат	1	10	1	10
Модульна контрольна робота	1	60		60
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. Кожна модульна контрольна робота

містить 30 тестових завдань. Максимальна кількість балів за кожний модуль становить 100 балів

Критерії оцінювання підсумкового семестрового контролю

Підсумковий семестровий контроль з дисципліни **«**Ліцензування, атестація та сертифікація у сфері безпеки 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, A) 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, B) 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.

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 «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. Ліцензування господарської діяльності із технічного та криптографічного захисту інформації

Тема 1. Умови ліцензування господарської діяльності, пов’язаної із захистом інформації та інформаційних систем. Перелік законодавчих та нормативно-правових актів, що визначають провадження ліцензованої діяльності у галузі КЗІ та ТЗІ

Тема 2. Порядок ліцензування господарської діяльності у галузі КЗІ (крім послуг електронного цифрового підпису) та ТЗІ, за переліком, що визначається Урядом.

Тема 3. Ліцензійні умови ведення господарської діяльності, пов'язаної із захистом інформації та інформаційних систем. Форми документів.

Тема 4. Технічні та криптографічні засоби і комплекси, що можуть використовуватися в господарській діяльності із захисту інформації

МОДУЛЬ 2. Атестація та сертифікація у сфері об'єктів інформаційної діяльності.

Тема .5 Порядок творення технічної системи захисту інформації на об'єкті інформаційної діяльності. Перелік нормативних документів.

Тема 6. Порядок сертифікації технічних та криптографічних засобів що використовуються для захисту інформаційних ресурсів.

Тема 7. Порядок атестації комплексу захисту інформації на об'єкті інформаційної діяльності, де циркулює інформація з обмеженим доступом.

Тема 8 Експертиза у сфері ТЗІ. Експертний висновок. Сертифікат відповідності.

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 Ліцензування господарської діяльності із технічного та криптографічного захисту інформації						
1. Умови ліцензування господарської діяльності, пов'язаної із захистом інформації та інформаційних систем. Перелік законодавчих та нормативно-правових актів, що визначають провадження ліцензованої діяльності у галузі КЗІ та ТЗІ	14	4				10
2. Порядок ліцензування господарської діяльності у галузі КЗІ (крім послуг електронного цифрового підпису) та ТЗІ, за переліком, що визначається Урядом	17	4		3		10
3. Ліцензійні умови ведення господарської діяльності, пов'язаної із захистом інформації та інформаційних систем. Форми документів.	17	4		3		10
4. Технічні та криптографічні засоби і комплекси, що можуть використовуватися в господарській діяльності із захисту інформації	17	4		3		10

Модульна контрольна робота	2	2				
Разом за модуль	67	18		9		40
Змістовий модуль 2. Атестація та сертифікація у сфері об'єктів інформаційної діяльності.						
5 Порядок створення технічної системи захисту інформації на об'єкті інформаційної діяльності. Перелік нормативних документів.	14	4		3		10
6. Порядок сертифікації технічних та крипто-графічних засобів, що використовуються для захисту інформаційних ресурсів.	15	4				11
7. Порядок атестації комплексу захисту інформації на об'єкті інформаційної діяльності, де циркулює інформація з обмеженим доступом.	17	4		3		10
8 Експертиза у сфері ТЗІ. Експертний висновок. Сертифікат відповідності.	17	4		3		10
Модульна контрольна робота	2	2				
Разом за модуль	68	18		9		41
Разом всього	**135**	**36**		**18**		**81**

6.3. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		денна	заочна
1	Порядок одержання ліцензії на ТЗІ та КЗІ	3	
2	Оформлення документів на одержання ліцензії. Виконання ліцензійних умов.	3	
3	Первинна сертифікація і стандартизація технічного засобу захисту інформації.	3	
4	Порядок чергової атестації СЗІ на ОІД. Застосування несертифікованих засобів захисту інформації.	3	
5	Проведення експертизи системи технічного захисту у інформації. Експертний висновок. Сертифікат відповідності	3	
6	Проведення експертизи системи криптографічного захисту інформації. Експертний висновок.	3	
Разом		**18**	

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин	
		денна	заочна
1	Законодавчі та нормативно-правові акти, що визначають провадження ліцензованої діяльності у галузі криптографічного захисту інформації та технічного захисту інформації	16	

2	Нормативно-правова база державної експертизи у сфері ТЗІ	15	
3	Засоби ТЗІ, які мають експертний висновок про відповідність до вимог технічного захисту інформації	10	
4	Використання засобів ТЗІ, які не мають експертного висновку	10	
5	Створення КСЗІ в ІТС, які використовуються для надання послуг доступу до мережі Інтернет	8	
6	Регулювання процедур використання технічних та криптографічних засобів захисту інформації в умовах воєнного стану	12	
7	Правове регулювання захисту персональних даних громадян в умовах воєнного стану	10	
	Разом:	**81**	

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

Основну інформацію з дисципліни 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.

Положення про державну експертизу в сфері технічного захисту інформації. Затверджене наказом Адміністрації Держспецзвязку від 16.05.2007 №93 і зареєстроване в Міністерстві юстиції України 16 липня 2007 р. за №820/14087.

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