Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту

Кафедра управління інформаційною безпекою

1. Загальна інформація

Назва дисципліни	Комплексні системи захисту інформації
Статус дисципліни	Нормативна
Рівень вищої освіти, форма навчання	Перший (бакалаврський), денна форма
Освітньо-професійна програма	Управління інформаційною безпекою
Спеціальність	125 Кібербезпека
Рік навчання, семестр	4-й рік (7 семестр)
Мова викладання	українська
Викладач	Полотай Орест Іванович, к. т. наук, доцент кафедри управління інформаційною безпекою
E-mail	o.polotaj@ldubgd.edu.ua
Сторінка курсу в ВУ	http://virt.ldubgd.edu.ua/course/view.php?id=197
Консультації	Згідно розкладу консультацій кафедри управління інформаційною безпекою

2. Анотація до курсу

Курс являє собою цикл лекційних та лабораторних занять, присвячених вивченню основних понять та методів побудови комплексних систем захисту інформації (КСЗІ).

Основні знання, що їх повинні набути здобувачі освіти, стосуються таких розділів: вимоги до КСЗІ та її завдання, проектування та введення в дію КСЗІ в ІТС.

3. Мета і завдання курсу

3.1. Метою навчальної дисципліни є ознайомити здобувачів з етапами створення КСЗІ в інформаційно-телекомунікаційних системах (ІТС), а також вимогами щодо побудови та особливостями впровадження.

3.2. Завдання:

- ознайомлення з нормативно-правовими документами України, які визначають необхідність створення комплексної системи захисту інформації;
- формування знань структури КСЗІ та особливості її побудови на об’єктах інформаційної діяльності при обробці різних видів інформації з обмеженим доступом, зокрема для

державної таємниці, службової інформації та персональних даних (конфіденційна інформація);
- формування вмінь здійснювати заходи щодо проектування, впровадження та супровід КСЗІ в ІТС;
- формування і розвиток логічного мислення;
- вміння застосовувати вимоги вітчизняних і міжнародних документів, що стосуються сфери захисту інформації;
- формування вмінь самостійно здобувати, осмислювати і застосовувати знання, користуватись необхідною літературою.

3.3. Компетентності:

Загальні компетентності:

- ЗК02 Знання та розуміння предметної області та розуміння професії.

Спеціальні (фахові) компетентності:

- ФК3 Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах;
- ФК6 Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних(автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження;
- ФК7 Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.);
- ФК9 Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

3.4. Програмні результати навчання:

- РН08 Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;
- РН12 Розробляти моделі загроз та порушника;
- РН18 Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;
- РН21 Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно- телекомунікаційних (автоматизованих) системах;
- РН29 Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.

4. Формат і обсяг курсу

Формат курсу	Навчальний матеріал дисципліни структурований за модульним принципом і складається з двох змістових модулів, які є логічно завершеними, відносно самостійними, цілісними частинами, засвоєння яких передбачає проведення 11 лабораторних робіт та аналіз результатів їх виконання. В процесі вивчення курсу здобувачі вищої освіти також повинні брати активну участь в обговорені дискусійних питань, вирішувати індивідуально та у групі ситуативні завдання.
Обсяг дисципліни:	4,5 кредити / 135 академічних годин, з яких: лекцій 14 годин, лабораторних 28 годин, самостійної роботи 93 годин.
Форми навчання	лекції, лабораторні заняття, курсовий проект, консультації, самостійна робота (в тому числі виконання здобувачами освіти індивідуальних

завдань у поза аудиторний час з подальшою їх перевіркою на лабораторних заняттях).

5. Тематика та зміст курсу

Назви змістових модулів і тем	Кількість годин (денна форма)				
	усього	у тому числі			
		л	п	лаб	с.р.
1	2	3	4	5	6
Змістовний модуль 1. Вимоги до КСЗІ та її завдання.					
Тема 1. Загальні положення про комплексну систему захисту інформації. Етапи побудови КСЗІ.	19	2		4	13
Тема 2. Категоріювання.	19	2		4	13
Тема 3. Складання моделі порушника та загроз.	21	2		4	15
Тема 4. Критерії оцінки захищеності інформації в ІТС від НСД.	19	2		4	13
Змістовний модуль 2. Проектування та введення в дію КСЗІ в ІТС.					
Тема 5. Розроблення політики безпеки та технічного завдання та проекту КСЗІ в ІТС.	19	2		4	13
Тема 6. Комплектування та введення в дію КСЗІ.	19	2		4	13
Тема 7. Проведення державної експертизи КСЗІ.	19	2		4	13
Усього годин	**135**	**14**		**28**	**93**

6. Інформаційний обсяг навчальної дисципліни

Змістовий модуль 1. Вимоги до КСЗІ та її завдання.

Тема 1. Загальні положення про комплексну систему захисту інформації. Етапи побудови КСЗІ.
Основні визначення і поняття комплексної системи захисту інформації. Структура. Складові компоненти. Аналіз етапів побудови КСЗІ.

Тема 2. Категоріювання.
Основні визначення і поняття. Мета проведення. Види категоріювання. Види категорій. Порядок виконання роботи.

Тема 3. Складання моделі порушника та загроз.
Основні визначення. Класифікація порушників. Побудова моделі порушника. Основні визначення. Поняття загроз. Класифікація. Побудова моделі загроз. Класифікація технічних каналів витоку інформації. Несанкціонований доступ. Сутність. Види.

Тема 4. Критерії оцінки захищеності інформації в ІТС від НСД.
Види керування доступом. Набір функціональних послуг. Стандартні функціональні профілі захищеності для автоматизованих систем класу 1, 2, 3. Рівні гарантій. Вибір профілю захищеності залежно від призначення автоматизованих систем.

Змістовий модуль 2. Проектування та введення в дію КСЗІ в ІТС.
Тема 5. Розроблення політики безпеки та технічного завдання та проекту КСЗІ в ІТС.в ІТС.
Основні поняття та визначення. Дискреційна, мандатна та рольова політики безпеки. Оформлення політики безпеки. Складання плану захисту. Технічне завдання. Проект КСЗІ.
Тема 6. Комплектування та введення у дію КСЗІ.
Комплекс технічного захисту інформації. Комплекс засобів захисту від несанкціонованого доступу. Апаратні та програмні засоби захисту. Вибір операційної системи, АВПЗ і КЗЗ від НСД. Організація введення КСЗІ в дію.
Тема 7. Проведення державної експертизи КСЗІ.
Етапи проведення державної експертизи КСЗІ. Виконавці робіт. Документи державної експертизи.

7. Завдання для самостійного опрацювання

З метою закріплення отриманих практичних навиків, здобувачі освіти виконують індивідуальні завдання, які отримують в кінці лабораторних занять. Лабораторні завдання відображені у електронному освітньому середовищі «Віртуальний університет». Перевірка правильності виконання лабораторних завдань проводиться на наступному лабораторному занятті.

8. Методи навчання

Основні форми організації навчання: лекції, лабораторні заняття із поточним контролем виконання індивідуальних завдань та проведенням тематичних лабораторних робіт, курсовий проект, консультації.
Методи організації та здійснення навчально-пізнавальної діяльності:

- лекції – словесні та наочні методи навчання із елементами мозкового штурму;
- лабораторні завдання, курсовий проект – частково-пошуковий метод навчання (певні елементи матеріалу відомі, решта студенти здобувають самостійно виконуючи завдання, тощо);
- консультації – словесний та дискусійний методи.

9. Технічне й програмне забезпечення /обладнання

Комп’ютери на базі процесорів Intel Pentium Gold G5400, компоненти програмного забезпечення MS Office 365 (Teams, PowerPoint, Word), електронне освітнє середовище “Віртуальний університет”(на базі платформи Moodle).

10. Критерії оцінювання

Оцінювання результатів навчання здобувачів вищої освіти здійснюється відповідно до «Положення про організацію освітнього процесу у ЛДУ БЖД» https://ldubgd.edu.ua/sites/default/files/1_nmz/polozhennya_pro_organizaciyu_osvitnogo_procesu_ldu_bzhd_nova_redakciya_10.2020.pdf та «Положення про порядок та критерії оцінювання результатів навчання здобувачів вищої освіти у ЛДУ БЖД» https://ldubgd.edu.ua/sites/default/files/1_nmz/nakazy/polozh_ldubzhd_poryadok_ocinyuvannya_.pdf.

Поточний контроль

Поточний контроль проводитися у формі тестування та виконання лабораторних завдань. Оцінювання результатів поточного контролю здійснюється за національною (чотирибальною) шкалою. Результати поточного контролю (поточна успішність) враховуються викладачем при виставленні підсумкової оцінки за екзамен.

Вид робіт	Формат проведення та критерії оцінювання
Тестові завдання	Курсом передбачено проходження 2 тестових завдання та модульна контрольна робота у вишляді тестів. Критерії оцінювання тестів наведені у електронному курсі «Віртуального університету». За успішне виконання тестових завдань сумарно можна отримати до 17 балів. Наприкінці семестру питання тестових завдань винесені у екзаменаційний тест.
Лабораторна робота	Курсом передбачено виконання та захист 11-ти лабораторних робіт. Типові завдання та критерії оцінювання наведені у електронному курсі «Віртуального університету». За виконання кожної лабораторної роботи можна отримати до 3 балів.
Робота на практичному занятті; самостійна робота	Оцінювання здійснюється за національною (чотирибальною) шкалою, відповідно до Додатку Б «Положення про порядок та критерії оцінювання результатів навчання здобувачів вищої освіти у ЛДУ БЖД». За роботу на лабораторних заняттях протягом семестру можна отримати до 30 балів.

Підсумковий контроль
Семестровий контроль проводиться у формі екзамену. Допуск до семестрового контролю здійснюється за умови виконання здобувачем лабораторних робіт, успішно пройденими підсумковими тестами в середовищі «Віртуальний університет» та захисту курсового проекту. Екзамен **(максимально 50 балів)** складається із двох компонентів: тестування у електронному освітньому середовищі “Віртуальний університет” (максимум 15 балів) та розв'язуванні двох типових завдань по 15 балів кожна, які оцінюються: - 15 балів – студент правильно виконав завдання. - 10 - студент правильно виконав половину завдання. - 5 - студент правильно виконав окремі завдання завдання.

Підсумкова семестрова оцінка обчислюється як сума балів поточного та підсумкового контролю за 100-бальною шкалою і переводяться в національну (чотирибальну) шкалу (“відмінно”, “добре”, “задовільно”, “незадовільно”, для заліків – “зараховано”, “не зараховано”).

Підсумкові оцінки виставляються та вносяться до екзаменаційної відомості, залікової книжки (позитивні результати) здобувача в національній, 100-бальній шкалі та шкалі ЄКТС відповідно до співвідношень, поданих у наступній таблиці.

Шкала оцінювання результатів навчання здобувачів вищої освіти

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, диференційованого заліку, курсового проекту (роботи), практики	для заліку
91 – 100	**A**	відмінно	зараховано
81-90	**B**	добре	
71-80	**C**		
61-70	**D**	задовільно	
51-60	**E**		
36-50	**FX**	незадовільно	не зараховано
0-35	**F**		

11. Політика курсу

Виконання навчальних завдань і робота в курсі має відповідати вимогам «Кодекс академічної доброчесності та корпоративної культури ЛДУ БЖД» https://ldubgd.edu.ua/sites/default/files/1_nmz/nakazy/kodeks_akademichnoyi_dobrochesnosti_ta_korpo.pdf

Академічні очікування від здобувачів – своєчасне виконання завдань, передбачених силабусом дисципліни; обов'язкове відвідування і виконання практичних занять та завдань самостійної роботи.

Політика щодо термінів виконання завдань та ліквідації академічної заборгованості: терміни виконання завдань вказуються у електронному курсі «Віртуального університету». Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Відпрацювання академічної заборгованості з дисципліни можливо до дня проведення підсумкового контролю (відповідно до розкладу).

Недопущені до підсумкового контролю здобувачі освіти здійснюють перездачу в терміни, відведені для усунення академічної заборгованості у два етапи:

заборгованість із поточного контролю;

заборгованість із підсумкового контролю.

Ліквідація заборгованості поточного контролю відбувається шляхом проходження тестових завдань та виконання лабораторних робіт згідно із тематичним планом курсу. Ліквідація заборгованості з підсумкового контролю організовується в форматі перездачі екзамену.

Дотримання принципів академічної доброчесності: роботи (завдання) виконуються здобувачами самостійно, ідеї та ініціативи інших авторів використовуються лише при належно оформленному цитуванні.

Поведінка в аудиторії – неприпустимо запізнення та користування телефоном на заняттях, за винятком виконання громіздких обчисленнях та використанні додаткових програм в освітніх цілях; повага до думки інших колег; дотримання норм культури мовлення та ін.

12. Рекомендована література

12.1. Основна:

1. *Полотай О.І. Бойко К.* Програмно-технічний захист інформації за допомогою охоронної системи. Захист інформації в інформаційно-комунікаційних системах : зб. тез. ІІІ Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів. Львів, ЛДУ БЖД. – 2019. С. 76-78.

2. *Полотай О.І. Масюк Н.* Модель навмисних загроз інформаційної безпеки техногенного походження. Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції. – Черкаси, 2021. - С.46-48

3. *Полотай О.І. Масюк Н.* Профілі можливостей порушників інформаційної безпеки структурних підрозділів безпекових структур. Актуальні проблеми управління інформаційною безпекою держави: Збірник тез наукових доповідей XII Всеукраїнської науково-практичної конференції – К. 2021. – С. 92-96.

4. *Полотай О.І. Рожко Д.* Організаційно-технічні методи захисту інформації від несанкціонованого доступу. "Інформаційна безпека в сучасному суспільстві": збірник тез доповідей ІІІ Міжнародної науково-технічної конференції. – Львів: ЛДУ БЖД, 2018. – С. 52-53.

5. Полотай О.І., Кухарська Н.П. Аспекти інформаційної безпеки в управлінні безперервністю діяльності організації. Information Technology and Security. July-December 2019. Vol. 7. Iss. 2 (13), pp. 126-136.

6. *Антонюк О.А.* Основи захисту інформації в автоматизованих системах / О.А. Антонюк – К.: Вид-во «КМ академія», 2003. – 244 с.

7. *Домарєв В.В., Швець В.А., Шестакова В.В.* Організаційне забезпечення захисту інформації з обмеженим доступом. Навчальний посібник. – К.: НАУ, 2006. – 108 с.

8. *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.

9. *Дудатьєв А.В.* Інформаційна безпека. Навчальний посібник. – Вінниця: УНІВАР-Сум-Вінниця, 2009. – 240 с.

12.2. Додаткова:

1. Закон України «Про інформацію» від 02.10.1992 №2657-XII.
2. Закон України «Про захист персональних даних», від 01.06.2010 № 2297-VI.
3. Закон України «Про доступ до публічної інформації», від 13.01.2011.
4. Закон України "Про державну таємницю".
5. Закон України "Про Державну службу спеціального зв'язку та захисту інформації України".
6. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".
7. Закон України "Про захист інформації в автоматизованих системах" від 05.07.94
8. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.
9. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.
10. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».
11. НД ТЗІ 1.1.-002-99. Загальні положення захисту інформації в комп'ютерних системах від несанкціонованого доступу.
12. НД ТЗІ 2.5.-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Вказівки щодо розроблення технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
13. НД ТЗІ 1.4.-001-2000. Типове положення про службу захисту в автоматизованій системі.
14. НДТЗІ 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
15. НД ТЗІ 2.7.- 001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт.
16. НД ТЗІ 3.6.-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів механічного захисту інформації від несанкціонованого доступу.
17. НД ТЗІ 3.7.- 002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації.
18. НД ТЗІ 4.7.- 002-2001. Визначення захищеності мовної інформації від витоку акустичним і віброакустичним каналами. Методичні вказівки.

12.3. Інформаційні ресурси:

1. Віртуальний університет ЛДУ БЖД [Електронний ресурс]. — Режим доступу: http://virt.ldubgd.edu.ua/
2. Елкетронний курс «Комплексні системи захисту інформації». [Електронний ресурс] — Режим доступу: http://virt.ldubgd.edu.ua/course/view.php?id=197

Розглянуто на засіданні кафедри управління інформаційною безпекою
протокол від «___» _____ №___

Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту

РОЗРОБНИК
Доцент кафедри управління інформаційною безпекою
кандидат технічних наук

_____ Орест ПОЛОТАЙ
«___» _____ 20__ р.

ЗАТВЕРДЖЕНО
Завідувач кафедри управління інформаційною безпекою
доктор технічних наук, доцент

_____ Ростислав ТКАЧУК
«___» _____ 20__ р.

ПОГОДЖЕНО
Гарант освітньої програми «Управління інформаційною безпекою»
першого (бакалаврського) рівня вищої освіти

_____ Орест ПОЛОТАЙ
«___» _____ 20__ р.

ПОГОДЖЕНО
Заступник начальника навчально-наукового інституту цивільного захисту

_____ Ольга МЕНЬШИКОВА
«___» _____ 20__ р.

Дата актуалізації*					
Підпис					
Ім’я, прізвище завідувача кафедри					