Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту

Кафедра управління інформаційною безпекою

1. Загальна інформація

Назва дисципліни	Технології захисту інформації
Статус дисципліни	Нормативна
Рівень вищої освіти, форма навчання	перший (бакалаврський), денна форма
Освітньо-професійна програма	Комп'ютерні науки
Спеціальність	122 Комп'ютерні науки
Рік навчання, семестр	3-й рік (5 семестр)
Мова викладання	українська
Викладач	Полотай Орест Іванович, к. т. наук, доцент кафедри управління інформаційною безпекою Брич Тарас Богданович, 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=2688
Консультації	Згідно розкладу консультацій кафедри управління інформаційною безпекою

2. Анотація до курсу

Як навчальна дисципліна «Технології захисту інформації» забезпечує формування базових знань з інформаційних технологій, для можливості орієнтуватися у сучасних напрямках захисту інформації, адміністрування і управління безпекою, аналізу та налагодженню системи безпеки, автоматизації задач налагодження системи безпеки, оцінки безпеки інформаційних технологій, розробки політики інформаційної безпеки та створенню безпечного зовнішнього середовища.

Основні знання, що їх повинні набути здобувачі освіти, стосуються таких розділів: технічні каналів витоку інформації, шляхів деструктивного впливу на інформацію та засоби її обробки, застосування заходів та засобів, спрямованих на технічний захист інформації на об'єктах інформаційної діяльності, алгоритмів розробки та реалізації заходів захисту, у тому числі і заходів захисту відомостей з обмеженим доступом, що проявляються фізичними об'єктами, захист інформації при роботі з персональними комп'ютерами.

3. Мета і завдання курсу

3.1. Метою навчальної дисципліни є вивчення основних положень та принципів побудови та використання програмних та апаратно-програмних та технічних засобів забезпечення безпеки інформації у комп'ютерних системах та мережах, які розташовані на об'єкті інформаційної діяльності, типовихі загроз та методів боротьби із ними.

3.2. Завдання:

- вивчити основні загрози для цілісності даних;
- аналізувати, оцінювати і вибирати методи, сучасні програмно-апаратні інструментальні та обчислювальні засоби, технології, алгоритмічні та програмні рішення для ефективного виконання конкретних виробничих задач з програмної інженерії;
- вміти приймати організаційно-управлінські рішення в умовах невизначеності;
- набувати нові наукові і професійні знання, вдосконалювати навички, прогнозувати розвиток програмних систем та інформаційних технологій;
- нати, розуміти та володіти навиками проектування і реалізації засобів захисту інформації у відповідності з політикою безпеки інформаційної системи;

3.3. Компетентності:

Спеціальні (фахові) компетентності:

- СК14 Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури

3.4. Програмні результати навчання:

- РН15 Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

4. Формат і обсяг курсу

Формат курсу Навчальний матеріал дисципліни структурований за тематичним принципом і складається з восьми лекцій, які є логічно завершеними, відносно самостійними, цілісними частинами, засвоєння яких передбачає проведення 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: 3 кредити / 90 академічних годин, з яких: лекцій 16 годин, лабораторних 16 годин, самостійної роботи 58 годин.

Форми навчання лекції, лабораторні заняття, 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
Тема 1. Огляд безпеки системи.	10	2		2	6

Назви змістових модулів і тем	Кількість годин (денна форма)				
	усього	у тому числі			
		л	п	лаб	с.р.
1	2	3	4	5	6
Тема 2. Технології захисту інформації.	10	2		2	6
Тема 3. Технічні канали витоку інформації та шляхи їх блокування.	10	2			8
Тема 4. Моделі захисту. Захист пам'яті.	10	2			8
Тема 5. Використання паролів і механізмів контролю за доступом.	12	2		4	6
Тема 6. Основні шляхи забезпечення безпеки інформації. Засоби, методи і системи захисту інформації. Захист інформації в персональних комп'ютерах.	12	2		2	8
Тема 7. Основні принципи захисту інформації при підключенні до мережі Інтернет	14	2		4	8
Тема 8.. Захист інформації в персональних комп'ютерах.	12	2		2	8
Усього годин за семестр	90	16		16	58
Усього годин	**90**	**16**		**16**	**58**

6. Інформаційний обсяг навчальної дисципліни

Тема 1. Огляд безпеки системи.
Основні поняття. Захист інформації та його основні завдання. Поняття про інформацію з обмеженим доступом. Структура політики безпеки та її основні частини. Життєвий цикл розробки систем безпеки.

Тема 2. Технології захисту інформації.
Завдання захисту інформації. Проблеми захисту інформації в комп'ютерних системах. Види комп'ютерних злочинів. Причини поширення комп'ютерної злочинності. Аналіз шкідливого програмного забезпечення.

Тема 3. Технічні канали витоку інформації та шляхи їх блокування.
Поняття технічного каналу витоку інформації. Класифікація каналів витоку інформації. Технічні канали витоку акустичної (мовної) інформації. Параметричні технічні канали витоку інформації. Класифікація і характеристика технічних каналів перехоплення інформації при їїпередачі по каналам зв'язку. Класифікація і характеристика способів прихованого відеоспостереження і зйомки. Пасивні засоби захисту. Активні засоби захисту.

Тема 4. Моделі захисту. Захист пам'яті.
Аналіз умов функціонування та загроз інформації комп'ютерних системах та мережах. Побудова моделі загроз у сучасних комп'ютерних мережах та системах. Побудова моделі порушника у сучасних комп'ютерних мережах та системах. Організація захисту пам'яті в ПК. Засоби захисту памяті в персональній ЕОМ.

Тема 5. Використання паролів і механізмів контролю за доступом.
Формальні моделі доступу. Дискреційний та мандатний доступ до інформації. Аналіз захищеності сучасних операційних систем. Підсистема захисту в ОС Windows. Порівняння архітектури

Windows та Linux.

Тема 6. Основні шляхи забезпечення безпеки інформації. Засоби, методи і системи захисту інформації.

Засоби захисту інформації в комп'ютерних системах. Методи і системи захисту інформації. Методи ідентифікації і встановлення достовірності об'єктів і суб'єктів. Стратегія та архітектура захисту інформації. Політика безпеки інформації. Види забезпечення безпеки інформації.

Тема 7. Основні принципи захисту інформації при підключенні до мережі Інтернет

Міжмережеві екрани. NAT. Proxy-сервер. Антивірусний захист поштової системи.

Тема 8. Захист інформації в персональних комп'ютерах.

Особливості захисту інформації в ПК. Загрози інформації в ПК. Захист ПК від несанкціонованого доступу.

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 практичному занятті.

8. Методи навчання

Основні форми організації навчання: лекції, практичні заняття із поточним контролем виконання індивідуальних завданнь та проведенням тематичних лабораторних робіт, консультації.

Методи організації та здійснення навчально-пізнавальної діяльності:

- лекції – словесні та наочні методи навчання із елементами мозкового штурму;
- лабораторні завдання – 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, Excel, Maple), електронне освітнє середовище "Віртуальний університет"(на базі платформи Moodle), Statistica.

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 5 тестових завдань. Критерії оцінювання тестів наведені у електронному курсі «Віртуального університету». За успішне виконання тестових завдань сумарно можна отримати до 30 балів. Наприкінці семестру питання тестових завдань винесені у заліковий тест.
Робота на лабораторному 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 20 балів.

Підсумковий контроль
Семестровий контроль проводиться у формі екзамену. Допуск до семестрового контролю здійснюється за умови виконання здобувачем двох контрольних робіт та успішно (оцінка «3» та більше) пройденими підсумковими тестами в середовищі «Віртуальний університет». Залік **(максимально 50 балів)** складається із тестування у електронному освітньому середовищі “Віртуальний університет”. Тест складається з багаторівневих питань. Сюди відносяться тести у вигляді вибору однієї правильної відповіді, тести у вигляді відповідності та формату правильно/неправильно. Загалом на тестування винесено 60 тестових завдань. Для відповідей відводиться 80 хв.

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. *Бабак В.П.*, Корченко О.Г. Інформаційна безпека та сучасні мережеві технології. Англо-українсько-російський словник термінів, Київ: НАУ, 2003. - 670 с.
2. *Герасименко В.А., Малюк А.А.* Основы защиты информации. - М: МИФИ, 1997.-537 с.
3. *Зегжда Д.П., Ивашко А.М.* Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2000. - 452 с.
4. *Полотай О., Бойко К.* Програмно-технічний захист інформації за допомогою охоронної системи. Зб. тез. III Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів "Захист інформації в інформаційно-комунікаційних системах" (м. Львів, 28 листопада 2019 р.). Львів : ЛДУБЖД, 2019. С. 76–78..
5. *Полотай О., Довганик С.* SIEM-системи, як елемент аналізу та управління подіями CSOC. Матер. Всеукр. наук.-практ. Internet-конф. "Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті : стан, досягнення, перспективи розвитку" (м. Черкаси, 16–22 березня 2020 р.). Черкаси : ЧНУ ім. Б. Хмельницького, 2020. С. 60–61.
6. *Девянин П.Н.* Теоретические основы компьютерной безопасности. Учебное пособие для вузов / Девянин П.Н., Михальский О.О., Правиков Д.И. и др. - М.: Радио и связь, 2000.- 192 с.

12.2. Додаткова:

1. *Хорошко В.А., Чекатков А.А.* Методы и средства защиты информации / под ред. Ю.С.Ковтанюка – К.: Издательство Юниор, 2003. – 504 с., ил.

12.3. Інформаційні ресурси:

1. Технології захисту інформації [Електронний ресурс] / Полотай Орест Іванович. — Режим доступу: http://virt.ldubgd.edu.ua/course/view.php?id=2688

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

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 «Комп'ютерні науки» першого (бакалаврського) рівня вищої освіти

_____ Олександр ПРИДАТКО
«___» _____ 20__ р.

ПОГОДЖЕНО
Заступник начальника навчально-наукового інституту цивільного захисту

_____ Ольга МЕНЬШИКОВА
«___» _____ 20__ р.

Дата актуалізації*					
Підпис					
Ім'я, прізвище завідувача кафедри					