Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту

Кафедра управління інформаційною безпекою

1. Загальна інформація

Назва дисципліни	Захист програмного забезпечення та програмні методи захисту
Статус дисципліни	Нормативна
Рівень вищої освіти, форма навчання	Другий (магістерський), денна форма, заочна форма
Освітньо-професійна програма	Управління інформаційною безпекою
Спеціальність	125 Кібербезпека
Рік навчання, семестр	1-й рік (1 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=183
Консультації	Згідно з розкладом консультацій кафедри управління інформаційною безпекою

2. Анотація до курсу

“Захист програмного забезпечення та програмні методи захисту” є дисципліною, нормативною складовою навчального плану. Дана дисципліна формує професійні компетентності здобувачів вищої освіти, які навчаються на спеціальності 125 “Кібербезпека”.

У межах дисципліни висвітлюються основні способи захисту програмного забезпечення від несанкціонованого доступу, зміни коду та несанкціоонованого використання. становить вивчення основних положень та принципів побудови. Основу дисципліни становить використання програмних та апаратно-програмних засобів забезпечення безпеки програм та даних у комп’ютерних системах та мережах. Опанування сучасних технологій роботи із даними на рівні створення та налагодження програмного забезпечення, засвоєння та використання методів захисту даних та програмного забезпечення є необхідним компонентом підготовки кваліфікованого інженера-програміста (Software Engineer), системного архітектора (System Architect), архітектора програмного забезпечення (Software Architect)..

3. Мета і завдання курсу

3.1. Метою навчальної дисципліни є ознайомлення студентів з основними принципами, сучасними програмними засобами захисту інформації в автоматизованих системах (АС), оволодіння практичними методами захисту програмного забезпечення від різних типів загроз.

3.2. Завдання:
- отримання теоретичних знань та практичних навиків при розв'язанні типових задач забезпечення безпеки програмного забезпечення; знання основних проблем програмного захисту інформації; вміння використовувати отримані знання для правильного вибору рішень при розробці програмних засобів захисту інформації; формування вмінь самостійно здобувати, осмислювати і застосовувати знання, користуватися необхідною літературою.

3.3. Компетентності:
Загальні компетентності:
- ЗК01 Здатність застосовувати знання у практичних ситуаціях.
- ЗК05 Здатність до пошуку, оброблення та аналізу науково-технічної інформації з різних джерел.

Спеціальні (фахові) компетентності:
- ФК01 Здатність вибирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід.
- ФК02 Здатність будувати та оцінювати на основі сучасних принципів, способів та методів теорії захищених систем моделі загроз, порушника, політики безпеки.
- ФК06 Здатність аналізувати та формулювати висновки для різних типів складних управлінських задач у наукових та ІТ організаціях.
- ФК08 Здатність до використання інформаційно комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
- ФК10 Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

3.4. Програмні результати навчання:

- РН01 Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
- РН05 Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;
- РН06 Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.
- РН13 Проводити атестацію режимних територій, приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.

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 чотирьох практичних робіт, тестування 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 32 годин, лабораторних 16 годин, самостійної роботи 42 години.

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 практичних заняттях), курсова робота.

5. Тематика та зміст курсу

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. Захист програмного забезпечення від несанкціонованого копіювання.												
Тема 1.1 Загальний огляд систем захис-ту програмного забезпечення.	11	4		2		5	14	2		2		10
Тема 1.2. Сучасний стан засобів подо-лання систем захисту програм-ного забезпечення.	11	4		2		5	10					10
Тема 1.3. Захист ПЗ від несанкціонова-ного копіювання методом прив'язки до комп'ютера.	11	4		2		5	10					10
Тема 1.4. Електрон-ні ключі захисту ПЗ від несанкціоно-ваного копіювання.	11	4		2		5	10					10
Змістовий модуль 2. Захист програмного забезпечення від несанкціонованого дослідження.												
Тема 2.1. Загальні принципу захисту програм від несанкціонованого дослідження.	11	4		2		5	14	2		2		10
Тема 2.2. Захист програм від дизасемблювання.	11	4		2		5	10					10

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Тема 2.3. Захист програм від налагоджування**.**	12	4		2		6	10					0
Тема 2.4. Сучасні технології дампінга і захисту від нього.	12	4		2		6	10					12
Усього годин	**90**	**32**	**0**	**16**		**42**	**90**	**4**		**4**		**82**

6. Інформаційний обсяг навчальної дисципліни

<u>Змістовий модуль 1.</u> Захист програмного забезпечення від несанкціонованого копіювання.
Тема 1.1. Загальний огляд систем захисту програмного забезпечення.
Мета і доцільність використання систем захисту. Класифікація системи захисту інформації. Основні алгоритми захисту програмного забезпечення. Показники застосовності та критерії оцінювання СЗПЗ. Основні вимоги до розробки систем захисту ПЗ. Розповсюджені типи захистів та їх недоліки: демо-версії програмного забезпечення, захист обмеженням часу роботи програми, захист, заснований на генерації серійного номера або на використанні зовнішнього “ключового файлу”, використання унікальних ідентифікаторів носія програмного продукту, навісні захисти, захисти за допомогою електронних ключів, надання розробникам ПЗ засобів SDK. Аналіз сучасних програмних продуктів для захисту програмного забезпечення.
Тема 1.2. Сучасний стан засобів подолання систем захисту програмного забезпечення.
Проблема існування засобів зламу захистів ПЗ. Класифікація засобів подолання СЗПЗ.
Тема 1.3. Захист ПЗ від несанкціонованого копіювання методом прив’язки до комп’ютера.
Прив’язка до вінчестера. Прив’язка до BIOS. Прив’язка до архітектури, до набору ПЗ і т.д. Вимірювання продуктивності апаратури. Метод з частковим стиранням пам’яті.
Тема 1.4. Електронні ключі захисту ПЗ від несанкціонованого копіювання.
Поняття електронного ключа, доцільність його використання. Будова електронного ключа. Класифікація електронних ключів за їх будовою. Класифікація електронних ключів за їх програмною частиною. Захист програм за допомогою електронного ключа. Методи зламу та протидії йому. Підвищення стійкості захисту. Можливості електронного ключа. Огляд та характеристика відомих ключів захисту. Перспективи розвитку електронних ключів. Правила використання електронних ключів.

<u>Змістовий модуль 2.</u> Захист програмного забезпечення від несанкціонованого дослідження.
Тема 2.1. Загальні принципу захисту програм від несанкціонованого дослідження.
Принципи побудови систем захисту та їх функції. Основні методи та засоби дослідження програм. Способи вбудовування захисних механізмів в ПЗ. Структура програм, захищених від дослідження.
Тема 2.2. Захист програм від дизасемблювання.
Необхідність і доцільність захисту від дизасемблювання. Основні методи протидії дизасемблюванню програм. Шифрування коду. Захист програм шляхом обфускації. Додаткові методи боротьби з автоматичними і інтерактивними дизасемблерами.

Тема 2.3. Захист програм від налагоджування.
Огляд і класифікація налагоджувачів. Захист від налагоджувачів реального режиму. Боротьба з налагоджувачами захищеного режиму. Додаткові прийоми антиналагоджувального програмування.
Тема 2.4. Сучасні технології дампінга і захисту від нього.
Порядок завантаження програми і виділення пам'яті процесу. Доступ до пам'яті та списку процесів. Отримання дампу пам'яті обраного процесу. Програми для знання дампу і захист від них. Деякі методи захисту від дампінгу.

7. Завдання для самостійного опрацювання

З метою закріплення отриманих практичних навиків, здобувачі освіти виконують індивідуальні завдання, які отримують в кінці практичного заняття. Практичні завдання відображені у електронному освітньому середовищі «Віртуальний університет». Перевірка правильності виконання практичних 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 тестових контрольних 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, розв'язуючи задачі 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).

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 п'яти тестових завдань. Критерії оцінювання тестів наведені у електронному курсі «Віртуального університету». За успішне виконання тестових завдань сумарно можна

	отримати до 25 балів. Питання тестових завдань винесені у екзаменаційний тест.
Робота на практичному занятті; самостійна робота	Курсом передбачено виконання чотирьох лабораторних робіт. 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 практичних 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 чотирьох лабораторних робіт та успішно пройденими підсумковими тестами в середовищі «Віртуальний університет». Екзамен **(максимально 55 балів)** складається з тестування у електронному освітньому середовищі "Віртуальний університет" (максимум 25 балів), та теоретичної частини, яка складається з двох питань (максимум 30 балів).

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 практичних 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. *Каплун В.А.* Захист програмного забезпечення. Частина 1 / Каплун В.А., Дмитришин О.В., Баришев В.Ю. – Вінниця : ВНТУ, 2005. – 140 с.
2. *Каплун В.А.* Захист програмного забезпечення. Частина 2 / Каплун В.А., Дмитришин О.В., Баришев В.Ю. – Вінниця : ВНТУ, 2014. – 105 с.

12.2. Додаткова:

1. *Варлатая С.К.* Аппаратно-программные средства и методы защиты информации : учеб. пособие / Варлатая С.К., Шаханова М.В. – Владивосток : Изд-во ДВГТУ, 2007. – 318 с.
2. *Зайцев А.П.* Программно-аппаратные средства обеспечения информационной безопасности : учеб. пособ. / Зайцев А.П., Голубятников И.В., Мещеряков Р.В., Шелупанов А.А. – М. : Машиностроение-1, 2006. − 260 с.
3. *Казарин О.В.* Теория и практика защиты программ / О.В. Казарин – М. : МГУЛ, 2004. – 450 с.
4. *Казарин О.В.* Безопасность программного обеспечения компьютерных систем / О.В. Казарин – М. : МГУЛ, 2003. – 212 с.
5. *Хорошко В.А.* Методы и средства защиты информации / Хорошко В.А., Чекатков А.А. – К. : Юниор, 2003. – 504с.
6. *Полотай О.І., Лагун А.Е.* Особливості приховування інформації в зображеннях з використанням молодшого значущого біта. Вісник ЛДУБЖД : зб. наук. праць. Львів : ЛДУБЖД, 2019. № 20. С. 17–22.
7. *Полотай О.І., Гриник Р.О.* Побудова інтелектуальної моделі криптоаналізу шифру Рабіна на базі генетичного алгоритму. Зб. тез доп. Міжнар. наук.- практ. конф. “Інформаційна безпека та комп’ютерні технології” (м. Кіровоград:, 24–25 березня 2016 р.). Кіровоград : КНТУ, 2016. С. 24–26.
8. *Полотай О., Сениш А.* Способи захисту ERP-систем. Зб. тез доп. IV Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів “Інформаційна безпека інформаційні технології” (м. Львів, 27 листопада 2020 р.). Львів : ЛДУБЖД, 2020. С. 17–19.
9. *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.
10. *Polotai O., Kukharska N., Lagun A.* The steganographic approach to data protection using arnold algorithm and the pixel-value differencing method. Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020. 2020. Article ID 9204108. P. 174–177.
11. *Polotai O., Belej O., Nestor N., Sadeckii J.* Features of Application of Data Transmission Protocols in Wireless Networks of Sensors. 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019. Proceedings. 2019. Article ID 8847878. P. 317–322.
12. *Polotai O.*, Belej O., Nestor N. Developing a local positioning algorithm based on the identification of objects in a Wi-Fi Network of the Mall. International Conference on Perspective Technologies and Methods in MEMS Designthis. 2019. Article ID 8817385. P. 32–36.

12.3. Інформаційні ресурси:

1. Віртуальний університет ЛДУ БЖД [Електронний ресурс]. — Режим доступу: http://virt.ldubgd.edu.ua/
2. Захист програмного забезпечення та програмні методи захисту [Електронний ресурс] / Полотай Орест Іванович. — Режим доступу: http://virt.ldubgd.edu.ua/course/view.php?id=183

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

РОЗРОБНИК
Доцент кафедри управління інформаційною безпекою, доцент

_____ Орест ПОЛОТАЙ
«___» _____ 20__ р.

ЗАТВЕРДЖЕНО
Завідувач управління інформаційною безпекою
доктор тематичних наук, доцент

_____ Ростислав ТКАЧКУК
«___» _____ 20__ р.

ПОГОДЖЕНО
Гарант освітньої програми «Управління інформаційною безпекою»
другого (магістерського) рівня вищої освіти

_____ Ростивлав ТКАЧУК
«___» _____ 20__ р.

ПОГОДЖЕНО
Заступник начальника навчально-наукового інституту цивільного захисту

_____ Ольга МЕНЬШИКОВА
«___» _____ 20__ р.

Дата актуалізації*					
Підпис					
Ім'я, прізвище завідувача кафедри					