Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту

Кафедра управління інформаційною безпекою

1. Загальна інформація

Назва дисципліни	Технології виявлення та аналізу шкідливого програмного забезпечення
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=3001
Консультації	Згідно з розкладом консультацій кафедри управління інформаційною безпекою

2. Анотація до курсу

“Технології виявлення та аналізу шкідливого програмного забезпечення” є дисципліною, нормативною складовою навчального плану. Дана дисципліна формує професійні компетентності здобувачів вищої освіти, які навчаються на спеціальності 125 “Кібербезпека”. Як нормативна складова, вивчення дисципліни дозволить слухачу сформувати індивідуальну освітню траєкторію.

Даний курс знайомить здобувачів вищої освіти з методами проведення зворотної розробки програмного забезпечення та апаратних пристроїв; основними фундаментальними поняттями і законами методів реверс інжинірингу для їх використання в сучасних умовах; принципами побудови сучасного програмного забезпечення; використанням основного математичного апарату та законів декомпіляції програмного забезпечення; використанням програмних засобів, які реалізують основні методи виявлення та аналізу шкідливих програм.

3. Мета і завдання курсу

3.1. Метою дисципліни є формування у майбутніх спеціалістів умінь та компетентностей для забезпечення професійних навиків, необхідних для подальшої роботи та застосуванню методів та засобів аналізу шкідливого програмного забезпечення в умовах широкого використання сучасних інформаційних технологій..

3.2. Завдання:

- вивчення класифікації та побудови типових ШПЗ
- вивчення принципів та систем ізоляції шкідливого програмного забезпечення за допомогою технологій віртуалізації різного рівня;
- вивчення складання та побудови програми з використанням мови асебмлера та машинного коду; вивчення аналізу ППЗ з використанням мови асебмлера, системної архитектури (ISA) та машинного коду.

3.3. Компетентності:

Загальні компетентності:

– ЗК2 Здатність проводити дослідження на відповідному рівні.
– ЗК4 Здатність оцінювати та забезпечувати якість виконуваних робіт.

Спеціальні (фахові) компетентності:

– ФК 3 Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.
– ФК 5 Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
– ФК 7 Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

3.4. Програмні результати навчання:

– РН 3 Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
– РН 4 Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
– РН 6 Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
– РН 10 Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
– РН 12 Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
– РН 23 Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

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 трьох тестових завдань, п'яти 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 32 години, практичних 16 годин, самостійної роботи 87 годин.

Форми навчання лекції, практичні заняття, консультації, самостійна робота (в тому числі виконання здобувачами освіти індивідуальних завдань у поза аудиторний час з подальшою їх перевіркою на практичних заняттях).

5. Тематика та зміст курсу

Назви змістових модулів і тем	Кількість годин (денна форма)					Кількість годин (заочна форма)				
	усього	у тому числі				усього	у тому числі			
		л	п	лаб	с.р.		л	п	лаб	с.р.
1	2	3	4	5	6	7	8	9	10	11
Змістовний модуль 1. Основи.										
Тема 1. Введення в аналіз шкідливих програм.	11	2	2		7	15	2		2	11
Тема 2. Статичний аналіз.	12	2	2		8	11				11
Тема 3. Динамічний аналіз.	12	2	2		8	11				11
Тема 4. Мова асемблера та дизасемблювання.	12	2	2		8	11				11
Тема 5. Дизасемблювання з використанням IDA.	12	2	2		8	11				11
Змістовний модуль 2. Практика.										
Тема 6. Налагодження шкідливих двійкових файлів.	12	2	2		8	16	2		2	12
Тема 7. Функціональні можливості шкідливого ПЗ та його персистентність.	12	4			8	12				12
Тема 8. Впровадження коду та перехоплення.	12	4			8	12				12
Тема 9. Методи обфускації шкідливих програм.	14	4	2		8	12				12
Тема 10. Полювання на шкідливі програми з використанням криміналістичного аналізу за дампами пам'яті.	12	4			8	12				12
Тема 11. Виявлення складних шкідливих програм із використанням криміналістичного аналізу дампів пам'яті.	14	4	2		8	12				12
Усього годин	**135**	**32**	**16**		**87**	**120**	**4**	**4**		**127**

6. Інформаційний обсяг навчальної дисципліни

Змістовий модуль 1. Основи.

Тема 1. Введення в аналіз шкідливих програм.

Що таке шкідливе ПЗ? Що таке аналіз шкідливих програм? Чому аналіз шкідливих програм? Типи аналізу шкідливих програм. Налаштування тестового середовища. Вимоги до середовища. Огляд архітектури тестового середовища. Встановлення та налаштування віртуальної машини Linux. Встановлення та налаштування віртуальної машини Windows. Джерела шкідливих програм.

Тема 2. Статичний аналіз.

Визначення типу. Визначення типу файлу за допомогою ручного методу. Визначення типу файлу за допомогою інструментальних засобів. Визначення типу файлу за допомогою Python. Зчитування інформації за допомогою цифрових відбитків. Генерування криптографічної хеш-функції з використанням інструментальних засобів. Визначення криптографічної хеш-функції у Python. Багаторазове антивірусне сканування Вилучення рядків. Визначення обфускування файлу. Перевірка інформації про PE-заголовок. Порівняння та класифікація шкідливих програм.

Тема 3. Динамічний аналіз.

Огляд тестового середовища. Системний та мережевий моніторинг. Інструменти динамічного аналізу (моніторингу). Етапи динамічного аналізу. Збираємо все разом: аналізуємо виконуваний файл шкідливого ПЗ. Аналіз бібліотеки (DLL, що динамічно підключається).

Тема 4. Мова асемблера та дизасемблювання.

Основи роботи із комп'ютером. Регістри процесора. Інструкції з передачі даних. Арифметичні операції. Побітові операції. Розгалуження та умовні оператори. Цикли. Опції. Масиви та рядки. Структури. Архітектура x64.

Тема 5. Дизасемблювання з використанням IDA.

Інструментальні засоби аналізу коду. Статичний аналіз коду (дизасемблювання) з використанням IDA. Дизасемблювання Windows API. Виправлення двійкового коду за допомогою IDA. Сценарії та плагіни IDA.

Змістовий модуль 2. Практика.

Тема 6. Налагодження шкідливих двійкових файлів.

Загальні налагодження концепції. Налагодження двійкового файлу за допомогою x64dbg. Налагодження двійкового файлу за допомогою IDA. Налагодження програми .NET.

Тема 7. Функціональні можливості шкідливого ПЗ та його персистентність.

Функціональні можливості шкідливого ПЗ. Методи персистентності шкідливих програм.

Тема 8. Впровадження коду та перехоплення.

Віртуальна. Режим користувача та режим ядра. Методи застосування коду. Методи перехоплення.

Тема 9. Методи обфускації шкідливих програм.

Просте кодування. Шкідливе шифрування. Користувацьке кодування/шифрування. Розпакування шкідливих програм.

Тема 10. Полювання на шкідливі програми з використанням криміналістичного аналізу за дампами пам'яті.

Етапи криміналістичного аналізу дампів пам'яті. Створення дампи пам'яті. Огляд Volatility. Перерахування процесів. Виведення списку дескрипторів процесу. Виведення списку DLL. Скидання виконуваного файлу та DLL. Виведення списку мережних підключень та сокетів. Перевірка реєстру. Перевірка служб. Вилучення історії команд.

Тема 11. Виявлення складних шкідливих програм із використанням криміналістичного аналізу дампів пам'яті.

Виявлення застосування коду. Вивчення застосування порожнього процесу. Виявлення перехоплення API. Руткіти у режимі ядра. Виведення списку модулів ядра. Обробка введення/виводу. Відображення дерева пристроїв. Виявлення перехоплення простору ядра. Зворотні виклики з ядра та таймери.

7. Завдання для самостійного опрацювання

З метою закріплення отриманих практичних навиків, здобувачі освіти виконують індивідуальні завдання, які захищають на практичних заняттях. Практичні завдання відображені у електронному освітньому середовищі «Віртуальний університет». Перевірка правильності виконання робіт проводиться на наступному практичному занятті.

8. Методи навчання

Основні форми організації навчання: лекції, практичні заняття із поточним контролем виконання індивідуальних завдань та проведенням тематичних тестових завдань, консультації.
Методи організації та здійснення навчально-пізнавальної діяльності:

- лекції – словесні та наочні методи навчання із елементами мозкового штурму;
- практичні 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 практичних завдань. Оцінювання результатів поточного контролю здійснюється за національною (чотирибальною) шкалою. Результати поточного контролю (поточна успішність) враховуються викладачем при виставленні підсумкової оцінки за диференційований залік.	
Вид робіт	**Формат проведення та критерії оцінювання**
Тестові завдання	Курсом передбачено проходження 3 тестових завдання. Критерії оцінювання тестів наведені у електронному курсі «Віртуального університету». За успішне виконання тестових завдань сумарно можна отримати до 15 балів. Питання тестових завдань винесені у заліковий тест.
Робота на практичному занятті; самостійна робота	Курсом передбачено виконання п'яти практичних робіт. За роботу на практичних заняттях протягом семестру можна отримати до 25 балів.

Підсумковий контроль
Семестровий контроль проводиться у формі заліку. Допуск до семестрового контролю здійснюється за умови виконання здобувачем практичних робіт та успішно пройденими підсумковими тестами в середовищі «Віртуальний університет». Залік **(максимально 60 балів)** складається із двох компонентів: тестування у електронному

освітньому середовищі “Віртуальний університет” та усному опитуванні.

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. *Козлов С.Е.* Теорія і практика боротьби з комп'ютерною злочинністю /В. О. Козлов. – М.: Гаряча лінія. – Телеком, 2012. — 176 с.
2. *Касперски К.* Техніка мережних атак. Прийоми протидії / К. Касперски. – — М.: Солон-Р, 2011. – 397с.
3. *Сердюк С.А.* Перспективні технології виявлення інформаційних атак/ В. А. Сердюк // Системи безпеки. – 2012. – № 5(47). – С. 96-97.
4. *Антимонов Ц.Р.* Інтелектуальні протистояння по лінії фронту Вірус-антивірус // Інформація і безпека: матеріали міжрегіональної науково-практ.конф. – Інформація і безпека. – Випуск 2. – Воронеж: ВДТУ, 2012. – С. 39-46.
5. *Мінаєв С.А.* Принципи організації протидії шкідливим програмам в інформаційно-телекомунікаційних системах на основі оптимізації їх функціонування / В. А. Мінаєв, С. В. Скриль // Радіосистеми. – Вип. 47 «Радіотехнічні і інформаційні системи охорони і безпеки». – Радіотехніка. – 2013. – №9. – С. 71-72.

12.2. Додаткова:

1. *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.
2. *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.
3. *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.
4. *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.
5. *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.

12.3. Інформаційні ресурси:

1. Віртуальний університет ЛДУ БЖД [Електронний ресурс]. — Режим доступу: http://virt.ldubgd.edu.ua/
2. Адміністрування інформаційних систем [Електронний ресурс] / Полотай Орест Іванович. — Режим доступу: http://virt.ldubgd.edu.ua/course/view.php?id=3001

Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту

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					