МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет інформаційних технологій і математики
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС
нормативного освітнього компонента

ДІАГНОСТИКА ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

підготовки бакалавра

спеціальності 125 Кібербезпека

освітньо-професійної програми Інформаційна безпека

Луцьк – 2022

Силабус навчальної дисципліни «Діагностика шкідливого програмного забезпечення**»** підготовки бакалавра, галузі знань 12 Інформаційні технології, спеціальності 125 Кіберебзпека, за освітньою програмою Інформаційна безпека

Розробник: Глинчук Л. Я., доцент кафедри комп'ютерних наук та кібербезпеки, кандидат фізико-математичних наук.

Погоджено
Гарант освітньо-професійної програми:

Глинчук Л.Я.

Силабус освітнього компонента затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

протокол № 2 від 29 вересня 2022 р.

Завідувач кафедри:  Гришанович Т. О.

І. Опис освітнього компонента

Найменування показників	**Галузь знань, спеціальність, освітньо-професійна** /освітньо-наукова/освітньо-творча **програма, освітній рівень**	**Характеристика освітнього компонента**
Денна (очна) форма навчання	12 Інформаційні технології 125 Кібербезпека Інформаційна безпека Бакалавр	**Нормативний**
		Рік навчання 2
Кількість годин/кредитів 135/4,5		**Семестр** 1-ий
		Лекції 30 год.
		Лабораторні 38 год.
ІНДЗ: немає		**Самостійна робота** 59 год.
		Консультації 8 год.
		Форма контролю: екзамен
Мова навчання		**Українська**

ІІ. Інформація про викладача

ПІП Глинчук Людмила Ярославівна
Науковий ступінь кандидат фізико-математичних наук
Вчене звання -
Посада доцент кафедри комп'ютерних наук та кібербезпеки
Контактна інформація номер моб. тел.: 095-890-4246,
ел. скринька: hlynchuk.ludmila@vnu.edu.ua
Дні занять http://194.44.187.20/cgi-bin/timetable.cgi?n=700

ІІІ. Опис освітнього компонента

1. Анотація освітнього компонента. Дисципліна «Діагностика шкідливого програмного забезпечення» належить до переліку нормативних навчальних дисциплін програми підготовки бакалавра за спеціальністю 125 «Кібербезпека». Спрямована на вивчення різного напряму шкідливого ПЗ, класифікації та особливості; виявлення (діагностику), контрзаходи та можливість захисту від нього. Передбачає ознайомлення з юридичними аспектами у випадках поширення, створення та використання шкідливого ПЗ.

2. Пререквізити. Знання та вміння, отримані в результаті вивчення дисциплін: «Сучасне програмне забезпечення та хмарні технології», «Вступ до фаху», «Нормативно-правова база кібербезпеки». Студенти повинні мати поняття про інформаційну безпеку та законодавство у сфері інформаційної безпеки, мати розуміння як користуватися спеціальним ПЗ для захисту інформації.
   Постреквізити. Знання та вміння, отримані в результаті вивчення дисципліни, можуть бути корисні: при вивченні дисциплін «Системи моніторингу загроз», «Захист

інформації в операційних системах», «Комплексні системи захисту інформації» та ін.; для того аби розуміти і вміти використовувати всі способи захисту та діагностики від усіх можливих видів шкідливого ПЗ.

3. Мета і завдання освітнього компонента. Мета дисципліни: розглянути різні види шкідливого ПЗ та їх класифікацію відповідно до напрямів: операційна система, мережа Інтернет, мобільні пристрої, персональні дані в електронній формі та ін; визначити способи діагностики та захисту від шкідливого ПЗ. Вирішувати задачі професійного напряму: виявлення шкідливого програмного коду або його слідів, аналіз функцій виявлених програм, аналіз способів установки та управління, формування висновку та алгоритму дій захисту (контрзаходів).

4. Результати навчання (Компетентності).
   КЗ 1. Здатність застосовувати знання у практичних ситуаціях.
   КЗ 2. Знання та розуміння предметної області та розуміння професії.
   КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.
   КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
   КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою та/або кібербезпекою.
   ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
   ПРН 4. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
   ПРН 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурнологічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
   ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
   ПРН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

5. Структура освітнього компонента.

Назви змістових модулів і тем	**Усього**	**Лек.**	**Лабор.**	**Сам. роб.**	**Конс.**	**Форма контролю / Бали**

Змістовий модуль 1. Види шкідливого програмного забезпечення						
Тема 1. Основні поняття: діагностика комп'ютера та шкідливе програмне забезпечення		2	4	4	2	ІРС/4,5
Тема 2. Класифікація шкідливого програмного забезпечення		2	2	4		ІРС/2
Тема 3. Інфекційне шкідливе ПЗ: віруси, стелси, троянські програми та ін.		2	4	4	2	ІРС/4
Тема 4. Інтернет-загрози та їх розповсюдження. Батьківський контроль		2	2	4		ІРС/2
Тема 5. Соціальна інженерія та прихований майнінг		2	2	4		ІРС/2
Тема 6. Загрози для мобільних телефонів та операційних систем		2	2	4		ІРС/2
Тема 7. Рекламне ПЗ, шпигунське ПЗ (клавіатурні логери та ін.), додзвонювач (діайлер), програми-вимагачі, шкідливі плагіни		2	2	4		ІРС/2
Разом за модулем 1	64	14	18	28	4	18,5
Змістовий модуль 2. Діагностика та захист від шкідливого програмного забезпечення						
Тема 8. Юридичні аспекти та відповідальність за створення, розповсюдження та використання шкідливого ПЗ		2	2	3		ІРС/2
Тема 9. Сучасні методи виявлення шкідливих програм: сигнатурний та евристичний аналіз (динамічний, статичний)		2	4	4	2	ІРС/4
Тема 10. Класифікації та види антивірусного ПЗ. Огляд найпоширенішого ПЗ даного типу		2	4	4		ІРС/4
Тема 11. Технології міжмережевих екранів та їх види. Показники захищеності міжмережевих екранів		2	2	4		ІРС/2,5
Тема 12. Методи боротьби зі шкідливим ПЗ засобами операційної системи		2	2	4		ІРС/2,5
Тема 13. Системи виявлення та запобігання вторгнень, їх класифікація. Система захисту інформації ЛОЗА		2	2	4		ІРС/2
Тема 14. Тестування на проникнення (pentesting). Огляд можливостей NMap, OpenVAS,		2	2	4	2	ІРС/2,5

Metasploit та онлайн інструментів						
Тема 15. Контрзаходи: моніторингові програмні продукти. SIEM-системи. Загальні правила для захисту від шкідливого ПЗ		2	2	4		IPC/2
Разом за модулем 2	71	16	20	31	4	21,5
Види підсумкових робіт						Бал
Модульна контрольна робота № 1 (тести)						20
Індивідуальна робота студента № 1						20
Індивідуальна робота студента № 2						20
Всього годин/Балів	135	30	38	59	8	100

6. Завдання для самостійного опрацювання.

№ з/п	**Тема (опрацювати)**
1	Види кібератак з мережі Інтернет
2	Особливості вірусів для різного виду операційних систем
3	Електронний документообіг та шкідливе програмне забезпечення
4	Утиліти прихованого адміністрування
5	Люки, логічні бомби, зомбі
6	"Жадібні" програми (greedy program)
7	Статичний та динамічний аналіз коду шкідливого ПЗ
8	Дослідження звітності антивірусних програм
9	Захист електронних фінансів
10	Загрози з боку ворожої країни в умовах війни
11	Виконання тестів на проникнення
12	Законодавство зарубіжних країн щодо шкідливого ПЗ
13	Опрацювання додаткових ресурсів та інтренет-джерел
14	Опрацювання практичного матеріалу та підготовка відповідей на питання до екзамену

IV. Політика оцінювання

Політика викладача щодо здобувача освіти

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку ВНУ імені Лесі Українки, загально-прийнятих моральних принципів, правил поведінки та корпоративної культури; підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності. Атмосфера на заняттях повинна бути творчою, відкритою до конструктивної критики. Недопустимі запізнення на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття; списування. Очікується, що всі студенти відвідають усі лекції і практичні заняття курсу.

Політика щодо академічної доброчесності

Дотримання академічної доброчесності здобувачами передбачає: самостійне виконання завдань поточного та підсумкового контролю (для осіб з особливим освітніми потребами ця вимога застосовується з урахуванням їх індивідуальних потреб і

можливостей); посилання на джерела інформації у разі використання ідей, тверджень, відомостей; дотримання норм законодавства про авторське право; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

Порушенням академічної доброчесності вважається: академічний плагіат, самоплагіат, фабрикація, фальсифікація, списування. За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності: повторне проходження оцінювання; повторне проходження відповідного освітнього компонента освітньої програми.

Під час модульного та підсумкового контролю (заліку) студентам заборонено користуються такими засобами як мобільний телефон, планшет, конспект, навчальна література, інші джерела інформації, в тому числі Інтернет-ресурси.

Політика щодо дедлайнів та перескладання

Усі передбачені завдання мають бути виконані у встановлений термін. Несвоєчасно виконані завдання оцінюються на нижчу оцінку. Виключенням можуть бути завдання, які не вдалося зробити з поважних причин, в такому випадку студент може доробити вказані завдання у вказаний термін.

Якщо здобувач вищої освіти був відсутній на заняттях з будь-якої причини, то він (вона) вивчає матеріал самостійно, використовуючи навчальні посібники, конспекти лекцій, матеріали дистанційного курсу, у випадку розміщення його на платформі дистанційного навчання Moodle, виконує всі домашні завдання. Прозвітуватися про виконання завдань можна, використовуючи дистанційний курс, прикріпивши виконанні завдання у відповідні комірки та попередити викладача про здане завдання, або під час консультацій або надіслати виконане завдання на корпоративну пошту викладача. Зворотній зв'язок з викладачем для з'ясування всіх питань: використання форуму, чату дистанційного курсу, корпоративної пошти університету або відповідної бесіди у певному месенджері.

Перескладання модульного контролю (письмового чи тестування) заборонено.

V. Підсумковий контроль

Підсумковий контроль з даної дисципліни передбачено у вигляді екзамену.

Оцінювання здійснюється за 100-бальною шкалою. Оцінка включає в себе поточний контроль та підсумковий модульний контроль. Максимальна кількість балів, яку може отримати студент під час поточного оцінювання за семестр – 40 балів. Підсумковий модульний контроль за семестр включає в себе оцінки за всі модульні контрольні роботи, тестові завдання, індивідуальну роботу студента і складає 60 балів. Якщо студент за період вивчення дисципліни набрав за поточний та модульний контроль мінімум 75 балів і погоджується із цим результатом, то оцінка за семестр може виставлятися без складання екзамену. В іншому випадку студент складає екзамен; максимальна кількість балів, яку можна отримати на екзамені – 60 балів, але бали за підсумковий модульний контроль анульовуються. Оцінка за семестр, у випадку складання екзамену, є сумою балів поточного контролю та балів, отриманих під час екзамену.

Порядок проведення екзамену – екзамен відбувається або у вигляді тестування (складається база питань за весь семестр) або у вигляді практичних завдань та усної відповіді на теоретичні питання.

VI. Шкала оцінювання

Шкала оцінювання знань здобувачів освіти з освітніх компонентів, де формою контролю є іспит

Оцінка	Лінгвістична оцінка	Оцінка за шкалою ECTS

в балах		оцінка	Пояснення
90–100	Відмінно	A	відмінне виконання
82–89	Дуже добре	B	вище середнього рівня
75–81	Добре	C	загалом хороша робота
67–74	Задовільно	D	Непогано
60–66	Достатньо	E	виконання відповідає мінімальним критеріям
1–59	Незадовільно	Fx	Необхідне перескладання

VII. Рекомендована література та інтернет-ресурси

1. Заплотинський Б.А. Основи інформаційної безпеки.Конспект лекцій. –КІВіП НУ “ОЮА”, кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. – 128 с.
2. Захист інформаційних ресурсів: навчально-методичний посібник до курсу “Захист інформаційних ресурсів” / укл. С. О. Троян. – Умань : [б.в.], 2012.-120 с.
3. Черкун О.М. Сучасні технології комп’ютерної безпеки. Монографія. Науковий керівник Р.М. Літнарович. МЕГУ, Рівне, 2012. – 90с.
4. Каплун В.А., Майданюк В.П. Д 81 Захист операційних систем. Навчальний посібник. – Вінниця: ВНТУ, 2006. – 180 с.
5. Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" // Відомості Верховної Ради України (ВВР), 2007 р., № 12, ст. 102.
6. Богуш В. М., Кривуца В. Г., Кудін А. М., «Інформаційна безпека: Термінологічний навчальний довідник» За ред. Кривуци В. Г. — Київ. 2004. — 508 с.
7. Цимбалюк В.С. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права // Кормич Б. А.
8. Харченко В. С. Інформаційна безпека. Глосарій. — К.: КНТ, 2005.
9. Організаційно-правові основи політики інформаційної безпеки України: Автореф. дис. д-ра юрид. наук: 12.00.07. — Х.: НХУ України, 2004.
10. Богуш В. М., Юдін О. К. «Інформаційна безпека держави». — К.: «МК-Прес», 2005. — 432с., іл.
11. Сідак В.С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС: Навчальний посібник / В.С. Сідак, В.Ю. Артемов. – К. : Вид-во КНТ, 2007. – 21-24 с.
12. Цимбалюк В.С. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права / В.С. Цимбалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К. : Вид-во НТУ України "КПІ", 2001. – № 4. – С. 43-48.

13. Краткое руководство по тестированию на проникновение. Сагар Рахалкар Пуна, Махараштра, Индия ISBN-13 (pbk): 978-1-4842-4269-8\ 玲 ISBN-13 (electronic): 978-1-4842-4270-4 https://doi.org/10.1007/978-1-4842-4270-4

Додаткова література (інтернет-джерела)

1. Шкідливе програмне забезпечення. [Електронний ресурс]. – Режим доступу до ресурсу: https://sites.google.com/site/zagrozu/project-updates
2. Постанова Верховної Ради України "Про прийняття за основу проекту Закону України про Концепцію державної інформаційної політики". [Електронний ресурс]. – Режим доступу до ресурсу: http://zakon1.rada.gov.ua/cgibin/laws/main.cgi?nreg=2897-17
3. Шкідливі програми, їх типи, принципи дії і боротьби з ними. [Електронний ресурс]. – Режим доступу до ресурсу: https://www.slideshare.net/Tania0408/ss-117466015
4. Шкідливі програми та віруси-вимагачі: у чому різниця? [Електронний ресурс]. – Режим доступу до ресурсу: https://uk.vpnmentor.com/blog/ шкідливі-програми-та-віруси-вимагачі/
5. Закон України "Про основні засади забезпечення кібербезпеки України" [Електронний ресурс]. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19#Text
6. Енциклопедія Інтернет-загроз [Електронний ресурс]. – Режим доступу до ресурсу: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/
7. Вірусна енциклопедія [Електронний ресурс]. – Режим доступу до ресурсу: https://zillya.ua/index.php?q=virus/virus_f
8. Аналіз WhisperGate. Частина 1 - Огляд ланцюга атаки. Статичний аналіз Trojan-Downloader (stage2.exe) [Електронний ресурс]. – Режим доступу до ресурсу: https://www.youtube.com/watch?v=QyVAeZ3hpX4&ab_channel=AlexanderAdamov
9. Аналіз WhisperGate. Частина 2 - Динамічний аналіз Stage2.exe. Симуляція Discord CDN із FakeNet-NG [Електронний ресурс]. – Режим доступу до ресурсу:https://www.youtube.com/watch?v=orzrnqx1OcM
10. Аналіз руйнівника CaddyWiper2. Частина 1 – декодування [Електронний ресурс]. – Режим доступу до ресурсу: https://www.youtube.com/watch?v=JvR6yh4QVus
11. Налаштування пісочниці (FLARE-VM) https://www.youtube.com/watch?v=8u1p_q47wyc

VII. Питання до екзамену

1. Як відбувається діагностика комп’ютера? Для чого вона потрібна?
2. Що таке програмна діагностика?
3. Що таке апаратна діагностика?
4. Що таке шкідливе ПЗ, шкідливий код, закладка?
5. Для чого використовують люки, логічні бомби?
6. Що таке "Жадібні" програми (greedy program)?
7. Інтернет-загрози та їх поширення.
8. Утиліти прихованого адміністрування.

9. Особливості соціальної інженерії.
10. Прихований майнінг.
11. Рекламне програмне забезпечення.
12. Клавіатурні логери та додзвонювачі.
13. Шпигунські програмні засоби.
14. Здирницькі програми, шкідливі плагіни.
15. Юридичні аспекти у сфері шкідливого програмного забезпечення.
16. Система виявлення вторгнень, класифікація.
17. Система запобігання вторгнень, класифікація.
18. Моніторингові програмні продукти: особливості та приклади використання.
19. Інфекційне програмне забезпечення: класифікація та особливості.
20. Як з'явились перші комп'ютерні віруси?
21. На чому заробляють автори комп'ютерних вірусів?
22. Складіть портрет сучасного хакера.
23. Чи пишуть антивірусні компанії віруси?
24. Як змінювалися комп'ютери за плином часу?
25. Які є типи шкідливого програмного забезпечення?
26. Опишіть основні джерела зараження шкідливим програмним забезпеченням.
27. «Хробак» – окремий вид шкідливих програм.
28. Як передається вірус? Що робить із зараженим файлом?
29. Назвіть основні джерела зараження ПК та мобільних пристроїв.
30. Що таке кібератака? Хто їх проводить? З якою метою?
31. Назвіть основні загрози направлені на мобільні пристрої.
32. Опишіть можливості троянської програми для мобільних пристроїв.
33. Розкажіть коротко історію розвитку мобільних вірусів.
34. Чи існують віруси для iOS? Хто їх розробляє?
35. Що ви знаєте про моделі роботи з платними послугами. Опишіть їх принцип роботи.
36. Назвіть основні способи захисту інформації у сучасному інформаційному світі.
37. Яким був перший антивірус? Опишіть як він працював.
38. Що таке евристичний аналізатор? Де використовується ця технологія?
39. Які існують класи антивірусів?
40. Як обрати кращий антивірус?
41. Що таке сигнатурний аналіз і як він відбувається?
42. Що таке евристичний аналіз і як він відбувається?
43. Що таке динамічний аналіз і як він відбувається?
44. Що таке статичний аналіз і як він відбувається?
45. Що таке пісочниця та як її налаштувати?
46. Що дає обфускація коду?
47. Опишіть як карають злочинців згідно законодавства у поширенні та використанні шкідливого ПЗ.
48. На які типи можна розділити фінансові дані якими можуть заволодіти зловмисники?
49. Назвіть найбільш розповсюджені способи отримання зловмисниками фінансової інформації.

50. Опишіть конкретні можливості захисту від втрати електронних фінансів.
51. Чим небезпечні скімери? Який захист від них найбезпечніший?
52. Дайте декілька конкретних порад для користувачів Android.
53. Опишіть особливості ОС для мобільних пристроїв.
54. Чим відрізняється ОС Android від iOS? Яка ОС більше схильна до вірусів?
55. Опишіть моделі тестування на проникнення.
56. Які етапи тестування на проникнення?
57. Що таке тестування на проникнення?
58. Які вбудовані засоби захисту має ОС (на прикладі конкретної).
59. Загальні правила для захисту від шкідливого програмного забезпечення.
60. Що таке батьківський контроль і для чого він використовується?
61. Опишіть відомі вам методи соціальної інженерії.