МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Східноєвропейський національний університет імені Лесі Українки
Кафедра національної безпеки

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної і навчальної роботи та рекрутації
проф. Гаврилюк С. В. _____
Протокол № 2 від «16» жовтня 2019 р.

№8016102019

ПРОГРАМА
вибіркової навчальної дисципліни

Діагностика шкідливого програмного забезпечення

підготовки бакалавра

галузі знань: 12 Інформаційні технології
спеціальності 125 Кібербезпека
освітньо-професійної програми (спеціалізації)Інформаційна безпека

Луцьк – 2019

Програма навчальної дисципліни“ДІАГНОСТИКА ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ” підготовки бакалавра, галузі знань 12 “Інформаційні технології”, спеціальності 125 “Кібербезпека”, за освітньо-професійною програмою (спеціалізацією) “Інформаційна безпека”.

Розробник: Глинчук Л. Я., кандидат фізико-математичних наук,старший викладач кафедри національної безпеки.

Рецензент: Кузьмич О. І., кандидат фізико-математичних наук, доцент кафедри комп’ютерної інженерії та кібербезпеки ЛНТУ

Рецензент:Булатецька Л. В., кандидат фізико-математичних наук, доцент кафедри прикладної математики та інформатики СНУ ім. Лесі Українки

Програма навчальної дисципліни затверджена на засіданні кафедри національної безпеки

протокол № ___ від _____ 2019 р.

Завідувач кафедри: _____(М. А. Наход)

Програма навчальної дисципліни схвалена науково-методичною комісією факультету історії, політології та національної безпеки

протокол № ____від _____ 2019 р.

Голова науково-методичної
комісії факультету _____(А. Г. Шваб)

Програма навчальної дисципліни схвалена науково-методичною радою Східноєвропейського національного університету імені Лесі Українки

1.ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітня програма, освітній ступінь</th><th>Характеристика навчальної дисципліни</th></tr>
<tr><td rowspan="2">Денна форма навчання</td><td rowspan="8">Галузь знань: 12 “Інформаційні технології” спеціальність 125 «Кібербезпека» освітньо-професійна програма (спеціалізація) “Інформаційна безпека” Освітній ступінь: бакалавр</td><td>Вибіркова</td></tr>
<tr><td>Рік навчання - 3</td></tr>
<tr><td rowspan="2">Кількість годин/кредитів
150/5</td><td>Семестр – 6</td></tr>
<tr><td>Лекції 30 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: немає</td><td>Практичні (семінарські) 30 год.</td></tr>
<tr><td>Самостійна робота 80 год.</td></tr>
<tr><td>Консультації 10 год.</td></tr>
<tr><td>Форма контролю: залік</td></tr>
</table>

2. АНОТАЦІЯ КУРСУ:

Дисципліна “ДІАГНОСТИКА ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ”належить до переліку вибіркових навчальних дисциплін програми підготовки бакалавра. Спрямована на вивчення різного напряму шкідливого ПЗ та можливість захисту від нього. Передбачає ознайомлення з юридичними аспектами у випадках поширення, створення та використання шкідливого ПЗ.

Мета навчальної дисципліни: розглянути різні види шкідливого ПЗ та їх класифікацію відповідно до напрямів: операційна система, мережа Інтернет, мобільні пристрої, персональні дані в електронній формі; визначити способи діагностики та захисту від шкідливого ПЗ.

Програмні результати навчання:

*Бакалавр повинен знати:*класифікацію шкідливого ПЗ; особливості шкідливого ПЗ для різних ОС; особливості шкідливого ПЗ в мережі Інтернет та його розповсюдження; шкідливе ПЗ у мобільних пристроях; електроні фінанси та шкідливе ПЗ; методи та способи захисту від шкідливого ПЗ різного виду; антивірусні програмні продукти; місце та роль моніторингових програмних продуктів у сфері діагностики шкідливого ПЗ; особливості використання систем

виявлення та запобігання вторгнень, їх класифікація; юридичні аспекти у сфері захисту інформації; загальні правила для захисту від шкідливого ПЗ.

Бакалавр повинен вміти: діагностувати появу шкідливого програмного забезпечення на ПК та мобільних пристроях; розуміти до якого виду відноситься знайдене шкідливе ПЗ; аналізувати та вибирати вірний метод захисту та боротьби зі шкідливим ПЗ; вірно перевіряти результат після знищення шкідливого ПЗ; використовувати законодавчу базу України для розуміння відповідальності за створення, поширення та використання шкідливого ПЗ.

3. КОМПЕТЕНЦІЇ

Загальні компетенції:

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.

Фахові компетенції:

КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.

КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

4. ІНФОРМАЦІЙНИЙ ОБСЯГ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Програма навчальної дисципліни складається з таких **змістових модулів**:

1. Види шкідливого програмного забезпечення.
2. Діагностика та захист від шкідливого програмного забезпечення.

Структура навчальної дисципліни представляється у вигляді таблиці 2.

Таблиця 2

Назви змістових модулів і тем	**Кількість годин**						
	Усього	**у тому числі**					
		Лек.	**Практ.**	**Лаб.**	**Інд.**	**Сам. роб.**	**Конс.**
1	2	3	4	5	6	7	8
Змістовий модуль 1. Види шкідливого програмного забезпечення							
Тема 1. Основні поняття: діагностика комп'ютера та шкідливе програмне забезпечення	10	2	2			6	
Тема 2. Класифікація шкідливого програмного забезпечення	12	2	2			6	2
Тема 3. Інфекційне шкідливе ПЗ: віруси, стелси, троянські програми та ін	12	2	2			6	2
Тема 4. Інтернет-загрози та їх розповсюдження	10	2	2			6	
Тема 5.Соціальна інженерія, прихований майнінг	10	2	2			6	
Тема 6. Загрози для мобільних телефонів та операційних систем	14	2	2			8	2
Тема 7. Рекламне ПЗ, клавіатурні логери, додзвонювачі	10	2	2			6	
Тема 8. Шпигунські програмні засоби, здирницькі програми, шкідливі плагіни	10	2	2			6	
Разом за модулем 1	88	16	16			50	6
Змістовий модуль 2. Діагностика та захист від шкідливого програмного забезпечення							

Тема 9.Юридичні аспекти та відповідальність за створення, розповсюдження та використання шкідливого ПЗ	8	2	2			4	
Тема 10. Антивіруси: технології, індустрія, практичне застосування	8	2	2			4	
Тема 11. Захист електронних фінансів	8	2	2			4	
Тема 12. Засоби захисту в мережі	10	2	2			4	2
Тема 13.Система виявлення та запобігання вторгнень, їх класифікація	8	2	2			4	
Тема 14. Контрзаходи: моніторингові програмні продукти	10	2	2			4	2
Тема 15. Загальні правила для захисту від шкідливого ПЗ	10	2	2			6	
Разом за модулем 2	62	14	14			30	4
Всього годин:	150	30	30			80	10

5. ЗАВДАННЯ ДЛЯ САМОСТІЙНОГО ОПРАЦЮВАННЯ

№ з/п	Тема	Кількість годин
1	Види кібератак з мережі Інтернет	**14**
2	Особливості вірусів для різного виду операційних систем	**12**
3	Електронний документообіг та шкідливе програмне забезпечення	**12**
4	Утиліти прихованого адміністрування	**14**
5	Люки, логічні бомби, зомбі	**14**
6	"Жадібні" програми (greedyprogram)	**14**
Разом		**80**

6. РОЗПОДІЛ БАЛІВ ТА КРИТЕРІЇ ОЦІНЮВАННЯ

Поточний контроль (max = 40 балів)					Модульний контроль (max = 60 балів)		Загальна кількість балів
Модуль 1					Модуль 2		
Змістовий модуль 1			Змістовий модуль 2		МКР 1	МКР 2	
Т1	Т2	Т3-Т8	Т9-Т12	Т13-Т15	40	20	100
2	2	3	3	2			

Шкала оцінювання (національна та ECTS)

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсової роботи (проекту), практики	для заліку
90 – 100	A	Відмінно	Зараховано
82 – 89	B	Добре	
75 – 81	C		
67 -74	D	Задовільно	
60 – 66	E		
1 – 59	Fx	Незадовільно	Незараховано (з можливістю повторного складання)

7. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна література

1. Захист інформаційних ресурсів: навчально-методичний посібник до курсу “Захист інформаційних ресурсів” / укл. С. О. Троян. – Умань : [б.в.], 2012.- 120 с.
2. Петров А.А. Построение комплексной системы защиты информации в сетях общего пользования. / Петров А.А. // Вісник СНУ ім. В.Даля. – 2009. - №136. – С. 135-143.

3. Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" // Відомості Верховної Ради України (ВВР), 2007 р., № 12, ст. 102.
4. Богуш В. М., Кривуца В. Г., Кудін А. М., «Інформаційна безпека: Термінологічний навчальний довідник» За ред. Кривуци В. Г. — Київ. 2004. — 508 с.
5. Цимбалюк В.С. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права // Кормич Б. А.
6. Хорев А.А. Способы и средствазащитыинформации. — М.: МО РФ, 2000. — 316 с.
7. Харченко В. С. Інформаційна безпека. Глосарій. — К.: КНТ, 2005.
8. С.Г. Лаптєва. — К.: Видавництво Європейського університету, 2001. — 201 с.
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. Жельников В. Криптография от папируса до компьютера. — М.: ABF, 1996. — 336с.
12. 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.
13. 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.

Додаткова література (інтернет-джерела)

1. Діагностика комп’ютера. [Електронний ресурс]. – Режим доступу до ресурсу: http://pkpartner.lviv.ua/services/diagnostics/#diagnostics
2. Шкідливе програмне забезпечення. [Електронний ресурс]. – Режим доступу до ресурсу: https://sites.google.com/site/zagrozu/project-updates
3. 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.

4. Шкідливі програми, їх типи, принципи дії і боротьби з ними. [Електронний ресурс]. – Режим доступу до ресурсу:https://www.slideshare.net/Tania0408/ss-117466015
5. Шкідливі програми та віруси-вимагачі: у чому різниця? [Електронний ресурс]. – Режим доступу до ресурсу: https://uk.vpnmentor.com/blog/шкідливі-програми-та-віруси-вимагачі/

8. ПЕРЕЛІК ПИТАНЬ ДО ЕКЗАМЕНУ

1. Діагностика комп’ютера та шкідливе програмне забезпечення.
2. Для чого використовують люки, логічні бомби?
3. Що таке "Жадібні" програми (greedyprogram)?
4. Інтернет-загрози та їх поширення.
5. Утиліти прихованого адміністрування.
6. Особливості соціальної інженерії.
7. Прихований майнінг.
8. Рекламне програмне забезпечення.
9. Клавіатурні логери та додзвонювачі.
10. Шпигунські програмні засоби.
11. Здирницькі програми, шкідливі плагіни.
12. Юридичні аспекти у сфері шкідливого програмного забезпечення.
13. Система виявлення вторгнень, класифікація.
14. Система запобігання вторгнень, класифікація.
15. Моніторингові програмні продукти: особливості та приклади використання.
16. Інфекційне програмне забезпечення: класифікація та особливості.
17. Як з’явились перші комп’ютерні віруси?
18. На чому заробляють автори комп’ютерних вірусів?
19. Складіть портрет сучасного хакера.
20. Чи пишуть антивірусні компанії віруси?
21. Як змінювалися комп'ютери за плином часу?
22. Які є типи шкідливого програмного забезпечення?
23. Опишіть основні джерела зараження шкідливим програмним забезпеченням.
24. «Хробак» – окремий вид шкідливих програм.
25. Як передається вірус? Що робить із зараженим файлом?
26. Назвіть основні джерела зараження ПК та мобільних пристроїв.
27. Що таке кібератака? Хто їх проводить? З якою метою?
28. Назвіть основні загрози направлені на мобільні пристрої.
29. Опишіть можливості троянської програми для мобільних пристроїв.

30. Розкажіть коротко історію розвитку мобільних вірусів.
31. Чи існують віруси для iOS? Хто їх розробляє?
32. Що ви знаєте про моделі роботи з платними послугами. Опишіть їх принцип роботи.
33. Назвіть основні способи захисту інформації у сучасному інформаційному світі.
34. Яким був перший антивірус? Опишіть як він працював.
35. Що таке евристичний аналізатор? Де використовується ця технологія?
36. Які існують класи антивірусів?
37. Як обрати кращий антивірус?
38. На які типи можна розділити фінансові дані якими можуть заволодіти зловмисники?
39. Назвіть найбільш розповсюджені способи отримання зловмисниками фінансової інформації.
40. Опишіть конкретні можливості захисту від втрати електронних фінансів.
41. Чим небезпечні скімери? Який захист від них найбезпечніший?
42. Дайте декілька конкретних порад для користувачів Android.
43. Опишіть особливості ОС для мобільних пристроїв.
44. Чим відрізняється ОС Android від iOS? Яка ОС більше схильна до вірусів?
45. Загальні правила для захисту від шкідливого програмного забезпечення.