(Ф 03.02 – 110)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний авіаційний університет
Факультет кібербезпеки, комп'ютерної та програмної інженерії
Кафедра безпеки інформаційних технологій

УЗГОДЖЕНО
Декан ФККПІ

_____ К. Нестеренко

«07» 09 2022 р.

ЗАТВЕРДЖЕНО
Проректор з навчальної роботи

_____ А. Полухін

«08» 09 2022 р.

Система менеджменту якості

РОБОЧА ПРОГРАМА
навчальної дисципліни

«Системи та технології виявлення уразливостей інформаційних систем»

Освітньо-наукова програма	«Кібербезпека»
Галузь знань	12 Інформаційні технології
Спеціальність:	125 Кібербезпека
Статус дисципліни:	вибірковий компонент
Освітній ступінь:	Доктор філософії

Форма навчання	Семестр	Усього (годин/кредитів ECTS)	Лекції	Практ. заняття	Лабор. заняття	Самостійна робота	Форма підсумк. контролю
Очна	4	150/5,0	20	30	-	100	Диф. залік
Заочна	4	150/5,0	6	10	-	134	Диф. залік

Індекс: РДФ - 4 - 125 / 22-2.1.2
Індекс: РДФ - 4 - 125 / 22-2.1.2 (З)

СМЯ НАУ РПНД 07.01.07-01-2022

Робочу програму навчальної дисципліни «Системи та технології виявлення уразливостей інформаційних систем» розроблено на основі освітньо-наукової програми «Кібербезпека», навчальних (№ НДФ - 4 - 125 / 22, № НДФ - 4 - 125 / 22(З)) та робочих навчальних (РДФ - 4 - 125 / 22, РДФ - 4 - 125 / 22(З)) планів підготовки здобувачів ступеня доктора філософії за спеціальністю 125 «Кібербезпека».

Робочу програму розробила:
доцент кафедри безпеки
інформаційної безпеки _____ Ю. Хохлачова

Робочу програму обговорено та схвалено на засіданні кафедри безпеки інформаційних технологій, протокол №7 від 22.08.2022 р.

Завідувач кафедри _____ О. Корченко

Робочу програму обговорено та схвалено на засіданні випускової кафедри освітньо-наукової програми підготовки докторів філософії «Кібербезпека», спеціальності 125 «Кібербезпека», кафедри безпеки інформаційних технологій, протокол №7 від 22.08.2022 р.

Завідувач кафедри _____ О. Корченко

Гарант освітньо-наукової програми _____ О. Корченко

Робочу програму обговорено та схвалено на засіданні науково-методично-редакційної ради факультету кібербезпеки, комп'ютерної та програмної інженерії, протокол №19 від «06» вересня 2022р.

Голова НМРР _____ С. Гнатюк

УЗГОДЖЕНО
Завідувач аспірантури та докторантури _____ А. Лелеченко
«07» 09 2022 р.

Рівень документа – 3б
Плановий термін між ревізіями – 1 рік
Контрольний примірник

АРКУШ ПОГОДЖЕННЯ

Гарант освітньо-наукової
програми «Кібербезпека» О. Корченко

ЗМІСТ

ВСТУП

Робоча програма (РП) навчальної дисципліни «Системи та технології виявлення уразливостей інформаційних систем» розроблена на основі Методичних рекомендацій щодо розроблення робочих програм навчальних дисциплін з підготовки здобувачів ступеня доктора філософії у Національному авіаційному університеті, затверджених наказом ректора від 29.04.2021р. №249/од.

1. ПОЯСНЮВАЛЬНА ЗАПИСКА

Мета та завдання навчальної дисципліни.

Дана навчальна дисципліна є однією з провідних в системі підготовки докторів філософії за ліцензованими в НАУ спеціальностями та спеціалізаціями, яка формує їх фаховий рівень та надає новітні методологічні основи з проведення наукових досліджень.

Мета та завдання є формування системи теоретичних знань та практичних умінь про сучасні наукові концепції, поняття, принципи і методики аналізу та опрацювання консолідованих інформаційних ресурсів та інженерії знань, що є практичною основою для фахівця в галузі кібербезпеки.

Завданнями вивчення навчальної дисципліни є:

- оволодіння технологіями моделювання інформаційних систем в умовах невизначеності;
- моделювання кіберресурсів;
- оволодіння механізмами кіберресурів із забезпеченням безпеки.

Очікувані результати навчання.

Навчальна дисципліна «Системи та технології виявлення уразливостей інформаційних систем» дає можливість досягти таких програмних результатів:

ПРН4. Здатність та уміння використовувати математичний апарат (теорії нечітких множин, математичної статистики, теорії імовірності тощо) для освоєння теоретичних основ, моделювання даних, практичного використання (обробки експериментальних даних), розробки нових та удосконалення існуючих методів, засобів та систем у сфері інформаційної та кібербезпеки.

ПРН5. Здатність проводити дослідження, розвиток та удосконалення сучасних моделей, методів, засобів та систем аналізу і оцінювання ризиків інформаційної та/або кібербезпеки при побудові комплексних систем захисту інформації, систем управління інформаційною безпекою, аудит стану кібербезпеки.

ПРН6. Здатність проводити дослідження, розвиток та удосконалення сучасних моделей, методів, засобів та систем аналізу і оцінювання негативних наслідків (шкоди) державі, суспільству, приватній чи юридичній особі у разі витоку державних інформаційних ресурсів, інформації з обмеженим доступом.

ПРН7. Здатність проводити дослідження, розвиток та удосконалення сучасних нейромережевих моделей, методів, засобів та систем виявлення нових загроз, мережевих кібератак, шкідливого програмного забезпечення, аналізу і оцінювання параметрів стану забезпечення активного захисту та кібербезпеки інформаційних (автоматизованих), інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури.

ПРН8. Здатність проводити дослідження, розвиток та удосконалення сучасних моделей, методів, засобів та систем виявлення вторгнень, визначати їх базові характеристики, а також обґрунтовано обирати та застосовувати в практичній роботі при побудові систем кібербезпеки.

ПРН9. Здатність продемонструвати знання та розуміння застосування методів, моделей та засобів ідентифікації аномальних станів для побудови систем виявлення вторгнень заснованих на теорії нечітких множин.

ПРН10. Вміти аналізувати, обґрунтовувати вибір та застосовувати методи фундаментальної та прикладної математики задля розв'язання задач аналізу, проектування і розробки елементів інтелектуальних систем кібербезпеки.

ПРН11. Здатність проводити дослідження, розвиток та удосконалення сучасних моделей, методів, засобів та систем кібербезпеки в умовах неповної визначеності.

Навчальна дисципліна «Системи та технології виявлення уразливостей інформаційних систем» дає можливість здобути такі компетентності:

ФК3. Здатність та уміння проводити дослідження теоретичних, науково-технічних і технологічних проблем, пов'язаних із організацією, створенням методів та засобів забезпечення захисту інформації та/або кібербезпеки при її зберіганні, обробці й передачі з використанням сучасних математичних методів, інформаційних технологій та технічних засобів.

ФК4. Здатність та уміння проводити дослідження проблеми забезпечення інформаційної безпеки національних інтересів України, вивчати і обґрунтовувати форми та методи захисту людини, суспільства й держави від зовнішніх і внутрішніх загроз в інформаційній сфері, а також шляхи підвищення ефективності функціонування інформаційних систем держави в сучасних умовах.

ФК5. Уміння застосовувати та розробляти сучасні технології, системи, технічні засоби, методи та моделі, бази даних та інші електронні ресурси, спеціалізоване програмне забезпечення у науковій, освітній та професійній діяльності;

ФК7. Здатність та уміння проводити дослідження проблеми забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів, інформаційні ресурси різних класів на об'єктах інформаційної діяльності та критичної інфраструктури, системи управління, на основі технології, методів, моделей та засобів у сфері інформаційної безпеки та/або кібербезпеки.

Передумови вивчення навчальної дисципліни.

Навчальна дисципліна «Системи та технології виявлення уразливостей інформаційних систем» базується на знаннях таких дисциплін, як: «Інноваційні методи прийняття рішень в соціотехнічних та соціокультурних системах», «Правове, економічне та інформаційне забезпечення наукових досліджень», «Методологія наукових досліджень у сфері кібербезпеки», «Наукові розробки та дослідження у сфері інформаційної безпеки та кібербезпеки (у т.ч. наукової школи «Кібербезпеки» НАУ)», «Теоретико-множинне моделювання даних для вирішення задач кібербезпеки/захисту інформації», «Англійська мова наукового спрямування», а результати навчання даного курсу можуть бути використані під час написання кандидатської дисертації.

2. ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Програма навчальної дисципліни.

Навчальний матеріал дисципліни структурований за модульним принципом і складається з одного навчального модуля, який є логічно завершеною, відносно самостійною, цілісною частиною навчальної дисципліни.

Модуль №1 «Системи та технології виявлення уразливостей інформаційних систем**»**

Інтегровані вимоги модуля №1:

Знати:

– Національну базу даних уразливостей, протокол автоматизації контенту та протокол документування та спільного використання структурної інформації про загрози.

– Банк даних загроз безпеки інформації, відомості про загрози ІБ та уразливості ПЗ, основні параметри загроз та уразливостей.

– Базу даних уразливостей від відкритих джерел, опис уразливостей, що заноситься в OSVDB та його інтерфейс;

– сучасні бази даних атак та їх використання в системах виявлення вторгнень.

Вміти:

– самостійно системно творчо мислити у досягненні мети професійної та науково-дослідницької діяльності при створенні технології клієнт-серверного програмного забезпечення надійного збереження даних;

– самостійно презентувати власні і колективні результати аналізу проблем кібербезпеки;

– самостійно вирішувати проблеми інноваційного характеру;

– самостійно шукати альтернативні рішення у професійній діяльності;

– самостійно креативно підходити до індивідуальної науково-дослідної діяльності;

– самостійно аналізувати, оцінювати та синтезувати нові ідеї;

– самостійно володіти навичками проведення експериментальних досліджень;

знання методології, методів та механізмів аналізу кіберресурсів із забезпеченням їх безпеки.

Тема 1.1. Національна база даних уразливостей (National Vulnerability Database)

Поняття База National Vulnerability Database. Протокол автоматизації контенту безпеки – Security Content Automation Protocol (SCAP). Протоколу документування та спільного використання структурної інформації про загрози.Threat Analysis Automation Protocol (TAAP), основні компоненти. Event Management Automation Protocol (EMAP) – протокол для звітів про події безпеки, основні складові. Incident Tracking and Assessment Protocol (ITAP) – протокол для відстеження, документування, управління та спільного використання інформації про інциденти, основні компоненти.

Тема 1.2. Банк даних загроз безпеки інформації. База даних уразливостей від відкритих джерел (Open Sourced Vulnerability Database).

Відомості про загрози ІБ та уразливості ПЗ. Основні параметри загроз та уразливостей. Також на сайті БДЗБІ міститься калькулятор CVSS v2.0. Основні відомості про базу уразливостей від відкритих джерел. Опис уразливості, що заноситься в OSVDB. Інтерфейс OSVDB.

Тема 1.3. Сучасні бази даних атак та їх використання в системах виявлення вторгнень. База даних уразливостей IBM X-Force.

Бази даних атак та їх структура. Набір даних NSL-KDD. База даних інцидентів веб-хакерства The Web Hacking Incident Database (WHID). База даних All.Net Security. Набір даних UNSW-NB15. Набори даних ADFA-LD та ADFA-WD. Бази даних атак, сформовані при проведенні конкурсів з кібербезпеки. Основні відмінності та особливості баз даних атак Особливості баз даних атак та їх використання в сучасних системах виявлення вторгнень. Основні відомості про базу даних уразливостей IBM X-Force. Приклад опису уразливості Microsoft Excel Remote Code Execution

Тема 1.4. База даних записів уразливостей US-CERT

Основні відомості про базу даних записів уразливостей US-CERT. Ідентифікатор «VU #». Основні пункти опису уразливості в VND. Приклад опису уразливостей. Вільні дані оцінок CVSS.

Тема 1.5. База даних уразливостей SecurityFocus. Бази шаблонів атак KDD-99 та CAPEC.

Основні відомості. Дослідження бази даних уразливостей SecurityFocus. Приклад опису уразливості Bugtraq 77270. Категорування баз даних на основі принципів теорії подібності. Опис параметрів мережевого з’єднання за базою шаблонів атак KDD-99. Структура шаблонів нормальної поведінки та кібератак за базою KDD Cup 1999. Структура бази CAPEC. Узагальнена схема формування джерел первинних даних для розроблення шаблонів потенційно небезпечних КбА.

Тематичний план навчальної дисципліни.

№ п/п	Назва теми	Обсяг навчальних занять (год.)							
		Очна форма навчання				Заочна форма навчання			
		Усього	Лекції	Практ./лабор. заняття (семінари)	СР	Усього	Лекції	Практ./лабор. заняття (семінари)	СР
1	2	3	4	5	6	7	8	9	10
Модуль №1 «Системи та технології виявлення уразливостей інформаційних систем**»**									
1.1	Національна база даних уразливостей (National Vulnerability Database).	**4 семестр**				**4 семестр**			
		27	4	3	20	23	1	2	20
1.2	Банк даних загроз безпеки інформації. База даних уразливостей від відкритих джерел (Open Sourced Vulnerability Database).	28	4	4	20	23	1	2	20
1.3	Сучасні бази даних атак та їх використання в системах виявлення вторгнень. База даних уразливостей IBM X-Force.	28	4	6	18	23	1	2	20
1.4	База даних записів уразливостей US-CERT	32	4	8	20	40	2	2	36
1.5	База даних уразливостей SecurityFocus. Бази шаблонів атак KDD-99 та CAPEC	32	4	8	20	41	1	2	38
1.6	Модульна контрольна робота №1	3	-	1	2	-	-	-	-
Усього за модулем №1		**150**	**20**	**30**	**100**	**150**	**6**	**10**	**134**
Усього за навчальною дисципліною		**150**	**20**	**30**	**100**	**150**	**6**	**10**	**134**

Лекційні заняття, їх тематика і обсяг

№ п/п	Назва теми	Обсяг навчальних занять (год.)			
		Очна форма навчання		Заочна форма навчання	
		Лекції	СРС	Лекції	СРС
1	2	3	4	5	6
1.1	Національна база даних уразливостей (National Vulnerability Database).	**4 семестр**		**4 семестр**	
		4	10	1	10
1.2	Банк даних загроз безпеки інформації. База даних уразливостей від відкритих джерел (Open Sourced Vulnerability Database).	4	10	1	10
1.3	Сучасні бази даних атак та їх використання в системах виявлення вторгнень. База даних уразливостей IBM X-Force.	4	10	1	10
1.4	База даних записів уразливостей US-CERT	4	10	2	18
1.5	База даних уразливостей SecurityFocus. Бази шаблонів атак KDD-99 та CAPEC	4	10	1	19
1.6	Модульна контрольна робота №1	-	1	-	-
Усього за модулем №1		**20**	**51**	**6**	**67**
Усього за навчальною дисципліною		**20**	**51**	**6**	**67**

Самостійна робота аспірантів

Самостійна робота з дисципліни складається з таких видів роботи:
1). опрацювання лекційного матеріалу;
2). підготовка до практичних занять;
3). підготовка до модульних контрольних робіт.

Завдання 1) виконується з метою поглиблення знань з лекційного матеріалу та полягає в опануванні більш широкого кола питань за тематикою лекцій.

Завдання 2) виконується з метою надбання практичних навичок з розробки та застосування технологій моделювання кіберресурсів та інформаційних систем в умовах невизначеності та оволодіння механізмами кіберресурів із забезпеченням безпеки.

Завдання 3) виконується з метою підготовки до продуктивної праці над тематикою модульної контрольної роботи та полягає у вивченні контрольних питань із затвердженого на засіданні кафедри переліку питань для підготовки до модульної контрольної роботи.

3. НАВЧАЛЬНО – МЕТОДИЧНІ МАТЕРІАЛИ З ДИСЦИПЛІНИ

Методи навчання

При вивчення навчальної дисципліни використовуються наступні методи навчання:
– пояснювально-ілюстративний метод;
– метод проблемного викладу;
– репродуктивний метод;
– дослідницький метод.

Реалізація цих методів здійснюється при проведенні лекцій, демонстрацій, самостійному вирішенні задач, роботі з навчальною літературою, аналізі та вирішенні задач з розробки та застосування методів виявлення аномальних станів породжених кібератаками. У процесі проведення лекційних занять використовуються мультимедійні технологій та пояснювально-ілюстративні методи навчання. Практичні заняття проводяться з використанням прикладного програмного забезпечення, роботи в групах та дослідницьких методів та методів проблемного викладення.

Рекомендована література

Базова

3.2.1 М.М. Браіловський, В.Д. Козюра, В.В. Кузавков, Ю.В. Пепа, Ю.М. Ткач, В.О. Хорошко Спеціалізовані програмні засоби наукових досліджень: навчальний посібник. – К.: ФОП Ямчинський О.В., 2022. – 204 с.

3.2.2. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с.

3.2.3. М.М. Браіловський, С.В. Зибін, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова. Технології захисту інформації: підручник. – К.: ЦП «Компринт», 2021. – 296 стр.

3.2.4. С.В. Зибін, В.В. Кузавков, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова. Стандартизація та правове забезпечення інформаційної безпеки: навчальний посібник. – К.: ЦП «Компринт», 2020. – 140 с.

3.2.5. Ю.В. Баланюк, В.В. Козловський, В.О. Хорошко, Ю.Є. Хохлачова. Інформаційно-психологічні впливи у кіберпросторі: навчальний посібник. – К.: ЦП «Компринт», 2020. – 109 с.

Допоміжна

3.2.6. Головань С.М. Загальне діловодство та ведення документів, що містять конфіденційну інформацію з грифом "Для службового користування". Навчально-методичний посібник. – К.: НАУ, 2003. – 92с.

3.2.7. Шевчук В.О., Корченко О.Г., Головань М.С., Душеба В.В., Пацира Є.В. Авіаційна безпека. Зберігання та обробка документів. Навчальний посібник. – К.: НАУ, 2004. – 92 с.

4. СИСТЕМА ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засоби оцінювання результатів навчальної діяльності.

Діагностика навчальних досягнень аспірантів здійснюється шляхомобов'язкового виконання аспірантами таких видів начальної діяльності:

- робота на практичному занятті;
- ділова гра;
- виконання модульної контрольної роботи.

Форми контролю результатів навчання та їх оцінювання

Оцінювання навчальної роботи аспіранта здійснюється в балах відповідно до табл. 4.1.

Таблиця 4.1

Вид навчальної діяльності	Максимальна кількість балів	
	Очна форма навчання	Заочна форма навчання
Модуль № 1 «Системи та технології виявлення уразливостей інформаційних систем»		
Діяльність 1	10б х 5 = 50	25б х 2 = 50
Діяльність 2	20	20
Модульна контрольна робота №1	30	х
Підсумкова контрольна робота	х	30
Поточна модульна оцінка №1	100	х
Всього за модулем № 1	**100**	**100**
Диференційований залік (за наявності)	**100**	
Підсумкова рейтингова оцінка	**100**	

Переведення підсумкової рейтингової оцінки в балах в оцінки за національною шкалою та шкалою ECTS здійснюється відповідно до табл. 4.2.

Таблиця 4.2.

Відповідність підсумкової рейтингової оцінки в балахоцінці за національною шкалою та шкалою ECTS

Оцінка в балах	**Оцінка за національною шкалою**	**Оцінка за шкалою ECTS**	
		Оцінка	**Пояснення**
90-100	**Відмінно**	**A**	**Відмінно** (відмінне виконання лише з незначною кількістю помилок)
82-89	**Добре**	**B**	**Дуже добре** (вище середнього рівня з кількома помилками)

75-81	**Добре**	**C**	**Добре** (в загальному вірне виконання з певною кількістю суттєвих помилок)
67-74	**Задовільно**	**D**	**Задовільно** (непогано, але зі значною кількістю недоліків)
60-66		**E**	**Достатньо** (виконання задовольняє мінімальним критеріям)
35-59	**Незадовільно**	**FX**	**Незадовільно** (з можливістю повторного складання)
1-34		**F**	**Незадовільно** (з обов'язковим повторним курсом)

Підсумкова рейтингова оцінка з дисципліни заноситься до заліково-екзаменаційної відомості, індивідуального навчального плану аспіранта та до академічної довідки про виконання освітньо-наукової програми.

Критерії оцінювання досягнень аспірантів.

Критерієм успішного проходження аспірантом оцінювання є досягнення ним мінімальних рівнів оцінок за кожним запланованим видом навчальної діяльності.

Виконані види навчальної роботи зараховуються аспіранту, якщо він отримав за них позитивну оцінку (за національною шкалою) відповідно до даних табл. 4.3.

Таблиця 4.3.

Відповідність рейтингових оцінок за окремі види навчальної роботи в балах оцінкам за національною шкалою[5]

Рейтингова оцінка в балах				**Оцінка за національною шкалою**
Оцінка за діяльність 1 (очна/заочна)	**Оцінка за діяльність 2**	**Модульна (підсумкова) контрольна оцінка**	**Поточна модульна оцінка**	
9-10 / 23-25	18-20	23-30	90-100	Відмінно
8 / 19-22	15-17	21-27	75-89	Добре
6-7 / 15-18	12-14	19-23	60-74	Задовільно
менше 6 / 15	менше 12	менше 19	менше 60	Незадовільно

Аспірант допускається до виконання модульної контрольної роботи за умови наявності у нього поточної модульної рейтингової оцінки величиною не менше 60% максимальної поточної модульної рейтингової оцінки.

Слід мати на увазі, що отримання аспірантом лише мінімальних оцінок за виконання окремих видів навчальної роботи з певного модуля може виявитися недостатнім для отримання допуску до виконання модульної контрольної роботи та потребуватиме виконання ним додаткового індивідуального завдання, захистити його з позитивною оцінкою в балах, яка буде додана до поточної модульної рейтингової оцінки.

До екзамену аспірант допускається за умови отримання позитивних (за національною шкалою) контрольних модульних рейтингових оцінок.

У разі отримання незадовільних контрольної модульної чи екзаменаційної рейтингових оцінок аспірант повинен повторно пройти відповідний контроль в установленому порядку. При повторному його проходженні максимальна величина рейтингової оцінки в балах не повинна перевищувати максимальне значення оцінки «Добре» за національною шкалою.

(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки

(Ф 03.02 – 02)

АРКУШ ОЗНАЙОМЛЕННЯ З ДОКУМЕНТОМ

№ пор.	Прізвище ім'я по-батькові	Підпис ознайомленої особи	Дата ознайом-лення	Примітки

(Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

№ пор.	Прізвище ім'я по-батькові	Дата ревізії	Підпис	Висновок щодо адекватності

(Ф 03.02 – 03)

АРКУШ ОБЛІКУ ЗМІН

№ зміни	№ листа (сторінки)				Підпис особи, яка внесла зміну	Дата внесення зміни	Дата введення зміни
	Зміненого	Заміненого	Нового	Анульо-ваного			

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				