Київський університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з наукової роботи
_____Наталія ВІННІКОВА
«___» _____ 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
ТЕХНОЛОГІЇ БЕЗПЕКИ
СКЛАДНИХ СОЦІОТЕХНІЧНИХ СИСТЕМ

для аспірантів

спеціальності 125 Кібербезпека та захист інформації
освітнього рівня третього (освітньо-наукового)
освітньо-наукової програми «Інформаційна безпека держави»

Київ – 2023

Розробники:

Бурячок Володимир Леонідович, доктор технічних наук, професор, завідувач кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка;

Коршун Наталія Володимирівна, доктор технічних наук, доцент, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Викладач:

Коршун Наталія Володимирівна, доктор технічних наук, доцент, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Протокол від 29.08.2023 р. № 8

Завідувач кафедри _____ Павло СКЛАДАННИЙ
(підпис)

Робочу програму погоджено з гарантом освітньо-наукової програми «Інформаційна безпека держави»

29.08.2023 р.

Гарант освітньо-наукової програми _____ Наталія КОРШУН
(підпис)

Робочу програму перевірено

29.08.2023 р.

Завідувач аспірантури, докторантури _____ Ілона ТРИГУБ
(підпис)

Пролонговано:

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	вибіркова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	3 / 90	
Рік навчання	2	2
Семестр	3	3
Кількість змістових модулів з розподілом:	3	
Обсяг кредитів	3	3
Обсяг годин, в тому числі:	90	90
Аудиторні	24	12
Модульний контроль	6	-
Самостійна робота	60	78
Форма семестрового контролю	залік	залік

2. Мета та завдання навчальної дисципліни

Метою викладання навчальної дисципліни «Технології безпеки складних соціотехнічних систем» є вивчення сучасного стану проблеми забезпечення безпеки в соціотехнічних системах (СТС), що визначається сукупністю взаємовідносин людини, інформаційної системи та навколишнього (оточуючого) середовища й залежить від впливу на них соціальних, економічних, політичних, природних, технічних та інших факторів.

Завдання полягає у:

- накопиченні аспірантами нових професійно профільованих знань і практичних навичок у галузі інформаційної та/або кібербезпеки, застосуванні їх для забезпечення захисту інформації в соціотехнічних системах;
- виявленні аспірантами проблемних аспектів у галузі забезпечення інформаційної та/або кібербезпеки, застосуванні їх для аналізу, оцінювання та вирішення завдань захисту інформації в соціотехнічних системах;
- формуванні у аспірантів здібностей до синтезу нових ідей, проведення наукових досліджень та реалізації технічних розробок у галузі інформаційної та/або кібербезпеки, застосуванні їх для продукування сучасних технологій захисту інформації в соціотехнічних системах.

3. Результати навчання за дисципліною

При вивченні дисципліни «Технології безпеки складних соціотехнічних систем» аспіранти повинні:

знати:

- основні загрози безпеки інформаційних систем;
- сучасні методи і науково-технічні рішення щодо забезпечення захисту інформації в СТС;

вміти:

- проводити оцінку безпеки СТС по заданому критерію;
- прогнозувати можливі витоки повідомлень в СТС;

- моделювати прості системи захисту;

оволодіти навичками:

- імовірнісного аналізу помилок в повідомленні;
- імовірнісного аналізу сумарних помилок на різних рівнях інформаційної взаємодії.

Спеціальні компетентності навчальної дисципліни:

СК-5 Здатність робити оцінки та в умовах припущень і обмежень знаходити відповідні рішення щодо систем інформаційної та/або кібербезпеки і захисту інформації

СК-6 Здатність до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки ІТ систем та мереж, обробки та перетворення інформації

СК-7 Здатність до планування і реалізації заходів із захисту інформації на об'єктах критичної інфраструктури, проведення моніторингу, аудиту та відновлення процесів штатного функціонування ІТ систем та мереж після збоїв та відмов різних класів і походження.

Результати навчання за дисципліною:

РН-5 - розробляти та аналізувати проекти ІКС базуючись на стандартизованих технологіях та протоколах передачі даних;
- аналізувати та визначати можливість застосування технологій, методів та засобів КТЗІ в ІКС;
- проектувати та реалізувати комплексні системи КТЗІ в ІКС відповідно до вимог чинних нормативно-правових документів системи захисту інформації;
- вирішувати задачі впровадження, супроводу та управління комплексними системами захисту інформації в ІКС, проведення їх експертизи та випробувань;
- забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту;

РН-6 - розробляти та впроваджувати дослідницькі проекти в сфері захисту інформації, інформаційної та кібербезпеки;
- розробляти алгоритми, моделі, методи та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки;
- здійснювати захист ресурсів і процесів в ІКС на основі моделей безпеки та встановлених режимів їх безпечного функціонування;
- забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту, виконувати розробку експлуатаційної документації на КЗЗ;
- забезпечувати функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками з врахуванням можливих конфліктів і катастроф;

РН-7 - вирішувати задачі централізованого і децентралізованого адміністрування доступом до ІР і процесів в ІКС та реалізовувати заходи з протидії отриманню несанкціонованого доступу до них;
- володіти науково-організаційними основами проведення аудиту безпеки ІКС, а також науковими методами та практичними навичками щодо створення систем моніторингу безпеки в ІТ системах та мережах.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Соціотехнічні системи: основні поняття, загрози і уразливості							
Тема 1. Складна соціотехнічна система: понятійний апарат та властивості	9	3					6
Тема 2. Основні уразливості складних соціотехнічних систем	9	3					6
Тема 3. Класифікація інформаційно-кібернетичних операцій на складні соціотехнічні системи. Їх математичне подання, стратегії і тактики їх застосування	8						8
Модульний контроль	2						
Разом	28	6					**20**
Змістовий модуль 2. Соціальний інжиніринг складних соціотехнічних систем							
Тема 4 Соціальна інженерія, як метод розвідки складних соціальних і соціотехнічних систем. Методи соціального інжинірингу	16		2	4			10
Тема 5 Загрози соціального інжинірингу. Алгоритм соціотехнічної атаки	16		2	4			10
Модульний контроль	2						
Разом	34		4	8			20
Змістовий модуль 3. Технологія оцінювання ефективності протидії атакам соціального інжинірингу та рівня захищеності складних соціотехнічних систем							
Тема 6 Соціоінженерні методи рішення проблем кібернетичної безпеки: тестування системи захисту інформації на проникнення	13	2		1			10
Тема 7. Технологія оцінювання ефективності протидії атакам соціального інжинірингу та рівня захищеності корпоративних IP від соціотехнічних атак	13	2		1			10
Модульний контроль	2						
Разом	28	4		**2**			**20**
Усього	**90**	**10**	**4**	**10**			**60**

Тематичний план для заочної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Соціотехнічні системи: основні поняття, загрози і уразливості							
Тема 1. Складна соціотехнічна система: понятійний апарат та властивості	10	1					9
Тема 2. Основні уразливості складних соціотехнічних систем	10	1					9
Тема 3. Класифікація інформаційно-кібернетичних операцій на складні соціотехнічні системи. Їх математичне подання, стратегії і тактики їх застосування	10	1		2			7
Модульний контроль							
Разом	30	3	-	2	-	-	25
Змістовий модуль 2. Соціальний інжиніринг складних соціотехнічних систем							
Тема 4 Соціальна інженерія, як метод розвідки складних соціальних і соціотехнічних систем. Методи соціального інжинірингу	12	1	1				10
Тема 5 Загрози соціального інжинірингу. Алгоритм соціотехнічної атаки	12	1	1				10
Модульний контроль							
Разом	24	2	2	-			20
Змістовий модуль 3. Технологія оцінювання ефективності протидії атакам соціального інжинірингу та рівня захищеності складних соціотехнічних систем							
Тема 6 Соціоінженерні методи рішення проблем кібернетичної безпеки: тестування системи захисту інформації на проникнення	18			2			16
Тема 7. Технологія оцінювання ефективності протидії атакам соціального інжинірингу та рівня захищеності корпоративних IP від соціотехнічних атак	18	1					17
Модульний контроль							
Разом	36	1	-	2			33
Усього	**90**	**6**	**2**	**4**			**78**

5. Програма навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ 1.
Соціотехнічні системи: основні поняття, загрози і уразливості.

Тема 1. Складна соціотехнічна система: понятійний апарат та властивості.

Базові поняття складних соціотехнічних й передусім інформаційно-телекомунікаційних систем. Концепція соціотехнічних систем. Системний підхід, як загально методологічний принцип створення складних соціотехнічних систем. Системний аналіз та синтез, як основні інструменти системного підходу.

Ключові слова: техніко-технологічні чинники, ефективність, керованість, стійкість, надійність, інформаційні відносини.

Тема 2. Основні уразливості складних соціотехнічних систем.

Основні уразливості соціотехнічних систем в умовах інформаційного протиборства. Інформаційна війна та зброя. Інформаційно-кібернетичні операції. Складові безпеки соціотехнічних систем. Модель системи захисту інформації в соціотехнічних системах.

Ключові слова: інформаційна війна, порушення, інформаційне протиборство.

Тема 3. Класифікація інформаційно-кібернетичних операцій на складні соціотехнічні системи. Їх математичне подання, стратегії і тактики їх застосування.

Основні класи загроз соціотехнічним системам за об’єктами мережевої взаємодії: атаки на прослуховування трафіку (спрямовані на порушення конфіденційності), атаки генерування об’єктів мережевої взаємодії (спрямовані на порушення цілісності), атаки з метою виведення з ладу мережевих пристроїв (спрямовані на порушення доступності).

Ключові слова: управління комплексною інформаційною безпекою, оцінювання інформаційної стійкості, логіко-ймовірнісна модель.

ЗМІСТОВИЙ МОДУЛЬ 2.
Соціальний інжиніринг складних соціотехнічних систем.

Тема 4. Соціальна інженерія, як метод розвідки складних соціальних і соціотехнічних систем. Методи соціального інжинірингу.

Розвідка складних соціальних і соціотехнічних систем. Основні сфери застосування соціальної інженерії. Технології соціального інжинірингу. Методи соціального інжинірингу за: взаємодією з політикою безпеки; дистанційністю; ініціалізацією; маніпулюванням; порушенням характеристик безпеки; реляційними ознаками; ступенем важкості; типом джерела; типом доступу.

Ключові слова: соціотехнічні атаки, методи соціального інжинірингу, маніпулювання, когнітивні упередження.

Тема 5. Загрози соціального інжинірингу. Алгоритм соціотехнічної атаки.

Етапи атаки соціального інжирірингу. Алгоритм Шейнова. Атаки типу фішингу (phishing) та його різновидів (вішинг, фармінг та ін.); претекстінгу (pretexting); аналізу «сміття»; особистісних підходів; реверсивної соціальної інженерії.

Ключові слова: соціальна інженерія, атака, фішинг, точка доступу, захист персональних даних, реверсивна соціальна інженерія.

ЗМІСТОВИЙ МОДУЛЬ 3.

Технологія оцінювання ефективності протидії атакам соціального інжинірингу та рівня захищеності складних соціотехнічних систем.

Тема 6. Соціоінженерні методи рішення проблем кібернетичної безпеки: тестування системи захисту інформації на проникнення.

Виявлення недоліків в області інформаційної безпеки (ІБ) з погляду сторонньої людини, які не були враховані при розробці політики безпеки. Розкриття і запобігання внутрішніх і зовнішніх спроб проникнення до соціотехнічних систем. Алгоритм дій при використанні технічних і соціоінженерних методів в ході проведення комплексного тесту на проникнення

Ключові слова: порушник, атака, експертна оцінка.

Тема 7. Технологія оцінювання ефективності протидії атакам соціального інжинірингу та рівня захищеності корпоративних ІР від соціотехнічних атак.

Алгоритм синтезу систем аналізу та оцінки рівня захищеності державних ІР від атак соціального інжинірингу. . Соціальний інжиніринг -це загроза безпеці інформації, заснована на отриманні певних даних (наприклад, імен користувачів, паролів, номерів телефонів віддаленого доступу тощо) від різних людей в процесі інформаційного обміну.

Ключові слова: оцінювання захищеності інформації, персонал, соціоінженерний підхід, ризик, оцінка ризику.

6. Контроль навчальних досягнень

Навчальні досягнення аспірантів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип пооперaційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу аспіранта на семінарських заняттях, за модульну контрольну роботу. Модульний контроль знань аспірантів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень аспірантів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, екзамен.
- *Комп'ютерного контролю:* тестові програми.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності аспірантів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

6.1 Система оцінювання навчальних досягнень аспірантів (денна форма)

Вид діяльності аспіранта	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2		Модуль 3	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	4	4	2	2	2	2
Відвідування семінарських занять	1	3	3	2	2		
Відвідування практичних занять	1			4	4	4	4
Відвідування лабораторних занять	1						
Робота на семінарському занятті	10	3	30	2	20		
Робота на практичному занятті	10			4	40	4	40
Лабораторна робота (в тому числі допуск, виконання, захист)	10						
Виконання завдань для самостійної роботи	5	2	10	2	10	2	10
Виконання модульної роботи	25	1	25	1	25	1	25
Разом		-	72	-	103		81
Максимальна кількість балів: 256							
Розрахунок коефіцієнта: 256/100=2,56							

Система оцінювання навчальних досягнень аспірантів (заочна форма)

Вид діяльності аспіранта	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2		Модуль 3	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	1,5	1,5	0,5	0,5	1	1
Відвідування семінарських занять	1					1	1
Відвідування практичних занять	1			1	1	1	1
Відвідування лабораторних занять	1						
Робота на семінарському занятті	10					1	10
Робота на практичному занятті	10			1	10	1	10
Лабораторна робота (в тому числі допуск, виконання, захист)	10						
Виконання завдань для самостійної роботи	5	2	10	2	10	2	10
Виконання модульної роботи							
Разом		-	11,5	-	21,5		33
Максимальна кількість балів: 66							
Розрахунок коефіцієнта: 66/100=0,66							

6.2 Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності аспіранта, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи аспіранта

№ з/п	Назва теми	Бали
Змістовий модуль 1. Соціотехнічні системи: основні поняття, загрози і уразливості		10
1	Складові соціотехнічних систем • виконання завдань відповідно до теми; • опрацювання фахових видань.	5
2	Захист інформації в соціотехнічних системах, як об'єкт адміністративно-правового та інженерно-технічного регулювання • виконання завдань відповідно до теми; • опрацювання фахових видань.	5
Змістовий модуль 2. Соціальний інжиніринг складних соціотехнічних систем		10
3	Методи соціального інжирнірингу • виконання завдань відповідно до теми; • опрацювання фахових видань.	5
4	Алгоритм соціального інжирнірингу: • виконання завдань відповідно до теми; • опрацювання фахових видань.	5
Змістовий модуль 3. Технологія оцінювання ефективності протидії атакам соціального інжинірингу та рівня захищеності складних соціотехнічних систем		10
5	Сутність організації ризикового режиму забезпечення ІКБ в складних соціотехнічних системах	5
6	Сутність и принципи міжнародного співробітництва в сфері безпеки складних соціотехнічних систем	5
	Разом	30

6.3 Критерії оцінювання самостійної роботи аспіранта

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

6.4 Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання аспірантів. Форма проведення – комп'ютерний тест, що складається 20 запитань закритої та відкритої форм.

Модульна контрольна робота оцінюється у 25 балів.

6.5. Форми проведення семестрового контролю

Семестровий контроль проводиться у вигляді заліку за результатами поточної успішності (проміжного контролю) з усіх змістових модулів дисципліни «Технології безпеки складних соціотехнічних систем».

6.6. Оцінювання освітніх досягнень аспірантів за системою ECTS

Рейтингова оцінка	Оцінка за стобальною шкалою	Значення оцінки
A	90-100 балів	Відмінно – відмінний рівень знань (умінь) в межах обов'язкового матеріалу з можливими незначними недоліками
B	82-89 балів	Дуже добре - достатньо високий рівень знань (умінь) в межах обов'язкового матеріалу без суттєвих (грубих) помилок
C	75-81 балів	Добре – в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74 балів	Задовільно - посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68 балів	Достатньо – мінімально можливий допустимий рівень знань (умінь)
FX	35-59 балів	Незадовільно з можливістю повторного складання – незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34 балів	Незадовільно з обов'язковим повторним вивченням дисципліни – досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Рекомендовані джерела

Основні:

1. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.: НАУ, 2013. – 432 с.

2. Ільяшов О.А., Бурячок В.Л. До питання захисту інформаційно-телекомунікаційної сфери від стороннього кібернетичного впливу // Наука і оборона. – 2010. – № 4. – С. 35–40.

3. Бурячок В.Л., Гулак Г.М., Хорошко В.О. Завдання, форми та способи ведення воєн у кібернетичному просторі // Наука і оборона. – 2011. – № 3. – С. 35–42.

4. Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень: монографія / Р. В. Грищук. – Житомир : Рута, 2010. – 280 с.

5. Бурячок В.Л. Алгоритм оцінювання ступеня захищеності спеціальних інформаційно-телекомунікаційних систем // Захист інформації. – 2011. – № 3(52). – С. 19–27.

6. Бурячок В.Л., Гулак Г.М., Хорошко В.О. До питання організації та проведення розвідки у кібернетичному просторі // Наука і оборона. – 2011. – № 2. – С. 19–23.

7. Бурячок В.Л., Корченко О.Г., Бурячок Л.В. Соціальна інженерія як метод розвідки інформаційно-телекомунікаційних систем // Захист інформації. – 2012. – № 4(57). – С. 5–12.

8.Бурячок В.Л., Бурячок Л.В., Костюк Т.Я. Обґрунтування вибору раціональної системи електронного документообігу для державних структур спеціального призначення // Вісник воєнної розвідки. – № 24. – 2011. – С. 67–74

10.Бондаренко Е. Соціальні мережі як інструмент розвитку- http://www.trainings.ru/library/articles/?id=10067

12.International Network for Social Network Analysis - http://www.insna.org/

14. Верховна Рада України. Законодавство України: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/

1. Державна служба спеціального зв’язку та захисту інформації: [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/index.

2. CERT-UA: [Електронний ресурс]. – Режим доступу: http://cert.gov.ua/.