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

СТРАТЕГІЇ НАУКОВИХ ДОСЛІДЖЕНЬ

Змістовий модуль

Сучасні технології інформаційної і кібербезпеки та захисту інформації

для аспірантів

спеціальності 125 Кібербезпека та захист інформації

освітнього рівня третього (освітньо-наукового)

освітньо-наукової програми «Інформаційна безпека держави»

Київ – 2023

Розробник:

Гулак Геннадій Миколайович, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:

Богданов Олександр Михайлович, доктор технічних наук, професор, 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 Факультету інформаційних технологій та математики
Протокол від 6.09.2023 №9

Завідувач кафедри _____ Павло СКЛАДАННИЙ
(підпис)

Робочу програму погоджено з гарантом освітньо-наукової програми «Інформаційна безпека держави»
06.09.2023

Гарант освітньо-наукової програми_____ Наталія КОРШУН
(підпис)

Робочу програму перевірено
06.09.2023

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)

1. Опис змістового модуля навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
СТРАТЕГІЇ НАУКОВИХ ДОСЛІДЖЕНЬ		
Вид дисципліни	Обов'язкова	
Мова викладання, навчання та оцінювання	Українська	
Загальний обсяг кредитів / годин	6 / 180, з них: Змістовий модуль «Сучасні технології інформаційної і кібербезпеки та захисту інформації» 2/60	
Рік навчання	1, 2	1, 2
Семестр	1, 2, 3	1, 2, 3
Кількість змістових модулів з розподілом:	5	5
Обсяг кредитів	6	6
Обсяг годин, в тому числі:	180	180
Аудиторні	48	24
Модульний контроль	12	
Самостійна робота	120	156
Форма семестрового контролю	Залік	Залік
Змістовий модуль «Сучасні технології інформаційної і кібербезпеки та захисту інформації»		
Рік навчання	2	2
Семестр	3	3
Кількість змістових модулів з розподілом:	1	1
Обсяг кредитів	2	2
Обсяг годин, в тому числі:	60	60
Аудиторні	16	8
Модульний контроль	4	-
Самостійна робота	40	52
Форма семестрового контролю	Залік	Залік

2. Мета та завдання змістового модуля «Сучасні технології інформаційної і кібербезпеки та захисту інформації» навчальної дисципліни «Стратегії наукових досліджень»

Мета: вивчення теоретичних та практичних напрацювань щодо забезпечення інформаційної і кібернетичної безпеки та захисту інформації; ґрунтовне ознайомлення студентів із методологією відповідних досліджень у галузі інформаційної безпеки та особливостями їх застосування в майбутній професійної діяльності.

Завдання полягає у наданні аспірантам теоретичних знань і практичних умінь у галузі проведення наукових досліджень та розробок сучасних систем та засобів інформаційної та кібербезпеки, а також захисту інформації.

У результаті вивчення змістового модуля «Сучасні технології інформаційної і кібербезпеки та захисту інформації» навчальної дисципліни «Стратегії наукових досліджень» відповідно до освітньо-наукової програми спеціальності формуються наступні компетентності:

загальні:

ЗК – 2 – здатність до нових професійно профільованих знань і практичних навичок та застосування їх в професійній діяльності;

ЗК-3 – здатність до виявлення профлемних аспектів у галузі забезпечення інформаційної та/або кібербезпеки, їх аналізу, оцінювання та вирішення;

ЗК-4 – Здатність до синтезу нових ідей, проведення наукових досліджень та реалізації технічних розробок за професійним спрямуванням н авідповідному рівні;

фахові:

СК-1 – Здатність оцінювати фізичні, технологічні, інформаційні, соціологічні, етичні та інші процеси інформаційного і кіберпросторів.

3. Результати навчання за дисципліною.

У результаті опрацювання змісту модуля «Сучасні технології інформаційної і кібербезпеки та захисту інформації» навчальної дисципліни «Стратегії наукових досліджень» здобувачі повинні:

знати: основні державні нормативні документи в галузі захисту інформації та міжнародні стандарти з інформаційної безпеки, процеси які висуваються ними при побудові захищених систем, особливості підтвердження відповідності побудованого захисту; принципи побудови систем забезпечення інформаційної безпеки; основні типи, призначення та характеристики сучасних технологічних рішень, направлених на забезпечення інформаційної безпеки;

вміти: використовувати на практиці нормативно-правові акти в галузі захисту інформації, державні та міжнародні стандарти з інформаційної безпеки; реалізовувати організаційні та технічні завдання, які виникають в процесі побудови систем інформаційної безпеки;

та досягти наступних *програмних результатів навчання:*

РН-2 – здійснювати інформаційний пошук; аналізувати потреби, пов'язані з науковими дослідженнями, з розвитком загальних компетентностей фахівців і професіоналів із захисту інформації, інформаційної та/або кібербезпеки; реалізовувати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, застосовуючи їх як в побуті, так і в професійній діяльності;

РН-3 – виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх в усній та/або письмових формах перед фаховою і нефаховою аудиторією;

РН-4 – забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів; здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосувати їх як в побуті, так і в професійній діяльності; проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД; обгрунтовувати раціональні шляхи щодо захисту інформації на ОІД та

інформації, що циркулює в ІТ системах та мережах; використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об’єктів інформаційної діяльності, а також наукових досліджень вищих рівнів.

4. Структура змістового модуля навчальної дисципліни.

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт		
		Аудиторна		Самостійна робота
		Лекції	Семінари	
ЗМІСТОВИЙ МОДУЛЬ «СУЧАСНІ ТЕХНОЛОГІЇ ІНФОРМАЦІЙНОЇ І КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ»				
Тема 1. Теоретичні та методологічні основи інформаційної і кібербезпеки та захисту інформації.	10	2	2	6
Тема 2. Стратегічні напрями забезпечення комп’ютерної безпеки та технічного захисту інформації в лініях і середовищах	10	2	2	6
Тема 3. Стратегічні напрями забезпечення комп’ютерної безпеки та технічного захисту інформації в лініях і середовищах	10	2	2	6
Тема 4. Перспективні напрями розвитку методів криптографічного захисту кіберпростору	12	2		10
Тема 5. Оцінка відповідності систем та засобів захисту інформації вимогам критеріїв та норм	14	2		12
Модульний контроль	4			
Разом	**60**	**10**	**6**	**40**

Тематичний план для заочної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт		
		Аудиторна		Самостійна робота
		Лекції	Семінари	
ЗМІСТОВИЙ МОДУЛЬ «СУЧАСНІ ТЕХНОЛОГІЇ ІНФОРМАЦІЙНОЇ І КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ»				
Тема 1. Теоретичні та методологічні основи інформаційної і кібербезпеки та захисту інформації.	10		2	8

Тема 2. Стратегічні напрями забезпечення комп'ютерної безпеки та технічного захисту інформації в лініях і середовищах	12		2	10
Тема 3. Концептуальні засади побудови апаратно-програмних комплексів мережі центрів реагування на кіберінциденти	12		2	10
Тема 4. Перспективні напрями розвитку методів криптографічного захисту кіберпростору	12	2		10
Тема 5. Оцінка відповідності систем та засобів захисту інформації вимогам критеріїв та норм	14			14
Разом	**60**	**2**	**6**	**52**

5. Програма змістового модуля «Сучасні технології інформаційної і кібербезпеки та захисту інформації» навчальної дисципліни «Стратегії наукових досліджень»

ЗМІСТОВИЙ МОДУЛЬ «СУЧАСНІ ТЕХНОЛОГІЇ ІНФОРМАЦІЙНОЇ І КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ»

Тема 1. Теоретичні та методологічні основи інформаційної і кібербезпеки та захисту інформації.

Сучасні моделі та концепції захисту інформація. Базові поняття методології наукових досліджень в сфері інформаційної і кібербезпеки та захисту інформації. Принципи, етапи, процеси і процедури забезпечення інформаційної і кібербезпеки та захисту інформації. Захист інформації як складова інформаційної і кібербезпеки (ІКБ) та його основні напрями. Євроатлантичні підходи до забезпечення ІКБ.

Основні поняття теми: розподілені мережі, інформаційна безпека, віртуалізація, IDS, SIEM, модель зрілості можливостей, мережеві технології; безпровідний зв'язок; ризики використання.

Тема 2. Стратегічні напрями забезпечення комп'ютерної безпеки та технічного захисту інформації в лініях і середовищах.

Розвиток методів і технологій блокування несанкціонованого доступу до інформації та її витоку. Проблеми та рішення убезпечення інформаційно-комунікаційних систем на основі хмарних технологій. Перспективні рішення щодо убезпечення інформаційно-комунікаційних систем: SEIM, IDS/IPS, антивірусний захист, безпека бездротового доступу, використання мобільних пристроїв і віддаленого доступу, оцінка ризиків, віртуальні приватні мережі (VPN), управління доступом.

Основні поняття теми: телекомунікаційні системи; антивірусний захист; обробка метаданих; хмарні антивірусні системи, соціальна інженерія; фішинг; хмарні сервіси; хмарні обчислення, нейронні мережі, системи виявлення вторгнень, віддалена робота; служби ІТ та ІБ.

Тема 3. Концептуальні засади побудови апаратно-програмних комплексів мережі центрів реагування на кіберінциденти.

Цілі та завдання центрів реагування на кіберінциденти (ЦРК). Архітектура апаратно-програмного комплексу ЦРК. Захищені протоколи взаємодії ЦРК. Технології оптимізації вибору та розміщення засобів захисту. Методи підвищення кіберкультури та кібергігієни користувачів інформаційних технологій.

Основні поняття теми: кібербезпека інформаційної системи, кластери станів безпеки;, коефіцієнт тяжкості наслідків, оптимальні стратегії фінансування, система підтримки прийняття рішень, багатокритеріальна оптимізація.

Тема 4. Перспективні напрями розвитку методів криптографічного захисту кіберпростору.

Проблеми та актуальні задачі постквантової криптографії. Технології блокчейн та електронні довірчі послуги в цифровому світі. Сучасні методи протидії шифрувальним вірусам. Тенденції розвитку криптопротоколів і криптоалгоритмів на основі еліптичних кривих.

Основні поняття теми: крива в узагальненому вигляді Едвардса, повна крива Едвардса, скручена крива Едвардса, квадратична крива Едвардса, порядок кривої, точковий порядок, ізоморфізм, ізогенія, рандомізація, стійка криптосистема, розподіл довжин повідомлень, критична інфраструктура, мобільний пристрій, криптоаналітична атака.

Тема 5. Оцінка відповідності систем та засобів захисту інформації вимогам критеріїв та норм.

Тренди розвитку критеріїв захищеності інформації, оцінок і індикаторів кібербезпеки, тестування та аудиту кібербезпеки/ кіберстійкості. Розвиток державної системи експертизи і оцінки відповідності у сфері захисту інформації. Сучасні тенденції сертифікації продукції у сфері захисту інформації на основі міжнародних стандартів.

Основні поняття теми: вектори атаки, несанкціонований доступ, сервіси хмарних обчислень, тестування на проникнення, об’єкт критичної інформаційної інфраструктури.

6. Контроль навчальних досягнень аспірантів.

6.1. Система оцінювання навчальних досягнень аспірантів (денна форма)

Вид діяльності аспіранта	Максимальна к-сть балів за одиницю	Модуль 3	
		Кількість одиниць	Максимальна кількість балів
Відвідування лекцій	1	5	5
Відвідування семінарських занять	1	3	3
Робота на семінарському занятті	10	3	30
Модульний контроль	25	2	50
Виконання завдань для самостійної роботи	5	5	25
Разом		100/113=0,88	
Коефіцієнт		0,88	

Система оцінювання навчальних досягнень аспірантів (заочна форма)

Вид діяльності аспіранта	Максимальна к-сть балів за одиницю	Модуль 3	
		Кількість одиниць	Максимальна кількість балів
Відвідування лекцій	1	1	1
Відвідування семінарських занять	1	3	3
Робота на семінарському занятті	10	3	30
Виконання завдань для самостійної роботи	5	15	75
Разом		100/109=0,91	
Коефіцієнт		0,91	

6.2.Завдання для самостійної роботи

ЗМІСТОВИЙ МОДУЛЬ «СУЧАСНІ ТЕХНОЛОГІЇ ІНФОРМАЦІЙНОЇ І КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ»

Самостійна робота є видом позааудиторної індивідуальної діяльності аспіранта, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності. В межах кожної теми аспіранти, використовуючи рекомендовану літературу, повинні

самостійно опрацювати джерела за запропонованою тематикою. Завдання для самостійної роботи подаються письмово. Кожна робота оцінюється від 1-5 балів.

Тема 1. Теоретичні та методологічні основи інформаційної і кібербезпеки та захисту інформації.

1. Характеристика інформації як предмета захисту
2. Потенційні загрози безпеки інформації та їх класифікація
3. Циклічна модель інформаційної безпеки

Тема 2. Стратегічні напрями забезпечення комп'ютерної безпеки та технічного захисту інформації в лініях і середовищах.

1. Захист інформації як об'єкт адміністративно-правового регулювання
2. Система органів регулювання технічного захисту інформації України.
3. Взаємодія суб'єктів системи технічного захисту інформації.
4. Напрями реалізації державної політики у сфері захисту інформації.

Тема 3. Концептуальні засади побудови апаратно-програмних комплексів мережі центрів реагування на кіберінциденти.

1. Державна експертиза у сфері захисту інформації.
2. Класифікація автоматизованих систем в НД ТЗІ.
3. Моделі захисту інформації в автоматизованій системі.
4. Модель порушника інформаційної безпеки.
5. Порядок і правила захисту інформації в АС.
6. Забезпечення конфіденційності, доступності й цілісності інформації в АС.

Тема 4. Перспективні напрями розвитку методів криптографічного захисту кіберпростору.

1. Криптосистеми та загрози їх безпеки.
2. Симетричні та асиметричні криптосистеми.
3. Формування та перевірка електронного цифрового підпису
4. Електронні довірчі послуги.
5. Порядок забезпечення криптографічного захисту інформації.

Тема 5. Оцінка відповідності систем та засобів захисту інформації вимогам критеріїв та норм.

1. Провідні світові та національні органи зі стандартизації.
2. Нормативне регулювання у сфері інформаційної безпеки в ЄС.
3. Підходи країн ЄС та НАТО щодо регулювання питань кібернетичної безпеки.
4. Сімейство стандартів інформаційної та кібернетичної безпеки.
5. Структура стандарту по кібербезпеці.
6. Базові блоки стандарту ISO 27032.
7. Заходи забезпечення кібербезпеки.
8. Основи обміну інформацією та координації.

Критерії оцінювання самостійної роботи

№ 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
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2
3	Дотримання вимог щодо технічного оформлення	1
	Разом	5

6.4. Форми проведення модульного контролю та критерії оцінювання

Модульний контроль проводиться у формі модульної контрольної роботи з урахуванням уніфікованої системи оцінювання навчальних досягнень аспірантів.

Критерії оцінювання модульного контролю наведено у таблиці.

Кількість балів	Критерії оцінювання
23-25 балів	Аспірант проявив глибокі систематичні знання даної теми, навів приклади, на переважну більшість питань дав правильну відповідь, допущені помилки є незначними.
19-22	Аспірант визначає структуру відповіді, допускає незначні помилки, що не впливають на загальний результат відповіді.
15-18	Аспірант орієнтується в питанні, проте не чітко формує структуру відповіді, допускає помилки, що порушують правильність відповіді.
10-14	Відповідь поверхнева, не змістовна.
7-9	Відповідь на примітивному рівні.
1-6	Аспірант не орієнтується в зазначеному питанні.

6.4. Форми проведення семестрового контролю

Семестровий контроль проводиться у вигляді заліку за результатами поточної успішності (проміжного контролю) зі змістового модуля дисципліни «Сучасні технології інформаційної і кібербезпеки та захисту інформації» навчальної дисципліни «Стратегії наукових досліджень».

6.5. 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 навчальної дисципліни – досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Рекомендована література

ЗМІСТОВИЙ МОДУЛЬ «СУЧАСНІ ТЕХНОЛОГІЇ ІНФОРМАЦІЙНОЇ І КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ»

Тема 1. Теоретичні та методологічні основи інформаційної і кібербезпеки та захисту інформації

Основна література:

1. Lakhno, V., Yerbolat, K., Bagdat, Y., Kryvoruchko, O., Desiatko, A., Tsiutsiura, S., & Tsiutsiura, M. (2022). Модель захисту локальної мережі навчального закладу серверної системи віртуалізації. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(18), 6-23. https://doi.org/10.28925/2663-4023.2022.18.623
2. Roy, Y., Riabchun, O., & Yermoshin , V. (2020). Модель зрілості можливостей системи кібербезпеки на об'єктах критичної інфраструктури енергетичного сектору ES-C2M2. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(10), 67-74. https://doi.org/10.28925/2663-4023.2020.10.6774
3. Opirskyy, I., Holovchak , R., Moisiichuk , I., Balianda , T., & Haraniuk , S. (2021). Проблеми та загрози безпеці IoT пристроїв. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(11), 31-42. https://doi.org/10.28925/2663-4023.2021.11.3142
4. Moshenchenko, M., & Zhurakovskyi, B. (2021). Захист інформації в технологіях "SMART CITY". Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(11), 100-109. https://doi.org/10.28925/2663-4023.2021.11.100109
5. Gnatyuk, S., Yudin , O., Sydorenko, V., & Yevchenko, Y. (2021). Метод формування функціонального профілю захищеності галузевих інформаційно-телекомунікаційних систем. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(11), 166-182. https://doi.org/10.28925/2663-4023.2021.11.166182
6. Laptiev, O., Sobchuk, V., Sobchuk, A., Laptiev, S., & Laptieva, T. (2021). Удосконалена модель оцінювання економічних витрат на систему захисту інформації в соціальних мережах. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(12), 19-28. https://doi.org/10.28925/2663-4023.2021.12.1928
7. Borsukovskyi, Y. (2019). Визначення вимог щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. частина 1. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(5), 61-72. https://doi.org/10.28925/2663-4023.2019.5.6172
8. Borsukovskyi, Y. (2019). Визначення вимог щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. частина 2. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(6), 112-121. https://doi.org/10.28925/2663-4023.2019.6.112121
9. Borsukovskyi, Y. (2020). Визначення вимог щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. частина 3. Електронне фахове

наукове видання «Кібербезпека: освіта, наука, техніка», 4(8), 34-48. https://doi.org/10.28925/2663-4023.2020.8.3448
10. Khlaponin, Y. I., Kondakova, S. V., Shabala, Y. Y., Yurchuk, L. P., & Demianchuk, P. S. (2019). Аналіз стану кібербезпеки в провідних країнах світу. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(4), 6-13. https://doi.org/10.28925/2663-4023.2019.4.613

Тема 2. Стратегічні напрями забезпечення комп'ютерної безпеки та технічного захисту інформації в лініях і середовищах

Основна література:

1. Pazynina, I., & Korchomnyi , R. (2022). Розробка рекомендацій щодо зниження кіберзагроз на час віддаленої роботи з точки зору кібербезпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 159-166. https://doi.org/10.28925/2663-4023.2022.17.159166
2. Ilyenko , A., Ilyenko , S., Kravchuk, I., & Herasymenko , M. (2022). Перспективні напрямки аналізу трафіку та виявлення вторгнень на основі нейромереж. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 46-56. https://doi.org/10.28925/2663-4023.2022.17.4656
3. Radivilova, T., Kirichenko, L., Tawalbeh, M., & Ilkov, A. (2021). Виявлення аномалій в телекомунікаційному трафіку статистичними методами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(11), 183-194. https://doi.org/10.28925/2663-4023.2021.11.183194
4. Drahuntsov , R., & Rabchun , D. (2021). Потенційні відволікаючі атаки на операційні центри безпеки та siem системи. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(14), 6-16. https://doi.org/10.28925/2663-4023.2021.14.614
5. Opirskyy, I., & Vynar , A. (2020). Аналіз використання хмарних сервісів для фішингових атак. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(9), 59-68. https://doi.org/10.28925/2663-4023.2020.9.5968
6. Smirnova, T., Polishchuk , L., Smirnov, O., Buravchenko, K., & Makevnin, A. (2020). Дослідження хмарних технологій як сервісів. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(7), 43-62. https://doi.org/10.28925/2663-4023.2020.7.4362
7. Tkachenko, O., Tkachenko, K., & Tkachenko , O. (2022). Хмарні технології у навчанні: онтологічний підхід. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 112-127. https://doi.org/10.28925/2663-4023.2022.17.112127
8. Smirnov, O. A., Smirnov, S. A., Polishchuk, L. I., Konoplitska-Slobodeniuk, O. K., & Smirnova, T. V. (2018). GERT-моделі технології хмарного антивірусного захисту. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(2), 6-30. https://doi.org/10.28925/2663-4023.2018.2.730
9. Shevchenko, S., Skladannyi, P., & Martseniuk, M. (2019). Аналіз та дослідження характеристик антивірусного програмного забезпечення, стандартизованого в Україні. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(4), 62-71. https://doi.org/10.28925/2663-4023.2019.4.6271

Тема 3. Концептуальні засади побудови апаратно-програмних комплексів мережі центрів реагування на кіберінциденти

Основна література:

1. Hulak, H., Skiter, I., & Hulak, Y. (2021). Методологічні засади створення та функціонування центру кібербезпеки інформаційної інфраструктури об'єктів ядерної енергетики. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(12), 172-186. https://doi.org/10.28925/2663-4023.2021.12.172186
2. Shemendiuk, O., Kozubtsov, I., Neshcheret, I., Protsiuk, Y., Bryhadyr, S., & Fomkin, D. (2022). Обрис функціонального призначення, потреб у складі обладнання і засобів комплексної апаратної зв'язку та кібербезпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(18), 61-72. https://doi.org/10.28925/2663-4023.2022.18.6172
3. Lakhno, V., Maliukov, V., Komarova, L., Kasatkin, D., Osypova, T., & Chasnovskyi, Y. (2022). Оптимізація розміщення засобів захисту інформації на основі застосування генетичного алгоритму. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 6-20. https://doi.org/10.28925/2663-4023.2022.17.620
4. Гулак, Г., & Лахно , В. (2019). Модель процесу інвестування в розвиток кібербезпеки для побудови системи підтримки прийняття рішень. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(6), 154-161. https://doi.org/10.28925/2663-4023.2019.6.154163
5. Chubaievskyi, V., Lakhno, V., Kryvoruchko, O., Kasatkin, D., Desiatko, A., Blozva, A., & Gusev, B. (2021). Методика мінімізації витрат на побудову багатоконтурної системи захисту на основі генетичного алгоритму. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(13), 16-28. https://doi.org/10.28925/2663-4023.2021.13.1628
6. Skiter, I. (2021). Модель оцінки рівня культури кібербезпеки в інформаційній системі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(13), 158-169. https://doi.org/10.28925/2663-4023.2021.13.158169
7. Arsenovych, L. (2022). Інструментарій підвищення рівня цифрової компетентності фахівців із кібербезпеки в освітньому процесі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(15), 93-109. https://doi.org/10.28925/2663-4023.2022.15.93109

Тема 4. Перспективні напрями розвитку методів криптографічного захисту кіберпростору

Основна література:

1. Bessalov, A., Kovalchuk, L., & Abramov , S. (2022). Рандомізація алгоритму CSIDH на квадратичних та скручених кривих Едвардса. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 128-144. https://doi.org/10.28925/2663-4023.2022.17.128144
2. Hulak, H., ZhdanovaY., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 145-158. https://doi.org/10.28925/2663-4023.2022.17.145158

3. Kulikovskyi, A. (2019). Технологія BLOCKCHAIN як складова інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(4), 85-89. https://doi.org/10.28925/2663-4023.2019.4.8589
4. Kurbatov, O., Kravchenko, P., Poluyanenko, N., Shapoval, O., & Kuznetsova, T. (2019). Децентралізована система ідентифікації та сертифікації. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(6), 19-31. https://doi.org/10.28925/2663-4023.2019.6.1931
5. Bebeshko, B. (2022). Аналіз методів та моделей прогнозування ринку цифрових криптовалют. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(18), 163-174. https://doi.org/10.28925/2663-4023.2022.18.163174
6. Hulak, H., Buriachok, V., Skladannyi, P., & Kuzmenko, L. (2020). Криптовірологія: загрози безпеки гарантоздатним інформаційним системам і заходи протидії шифрувальним вірусам. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(10), 6-28. https://doi.org/10.28925/2663-4023.2020.10.628

Тема 5. Оцінка відповідності систем та засобів захисту інформації вимогам критеріїв та норм

Основна література:

1. Lakhno, V., Blozva, A., Misiura , M., Kasatkin , D., & Gusev , B. (2020). Модель показника поточного ризику реалізації загроз інформаційно-комунікаційним системам. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(10), 113-122. https://doi.org/10.28925/2663-4023.2020.10.113122
2. Maltseva, I., Chernysh, Y., & Ovsiannikov, V. (2021). Аналіз методик оцінки кіберстійкості критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(12), 29-35. https://doi.org/10.28925/2663-4023.2021.12.2935
3. Litvinchuk, I., Korchomnyi , R., Korshun , N., & Vorokhob , M. (2020). Підхід до оцінювання ризиків інформаційної безпеки для автоматизованої системи класу «1». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(10), 98-112. https://doi.org/10.28925/2663-4023.2020.10.98112
4. Khlaponin, Y., Kozubtsova, L., Kozubtsov, I., & Shtonda, R. (2022). Функції системи захисту інформації і кібербезпеки критичної інформаційної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(15), 124-134. https://doi.org/10.28925/2663-4023.2022.15.1241341
5. Barchenko, N., Lubchak, V., & Lavryk, T. (2022). Модель індикаторів оцінки національного рівня цифровізації та кібербезпеки держав світу. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(18), 73-85. https://doi.org/10.28925/2663-4023.2022.18.7385
6. Tyshyk, I. (2022). Тестування корпоративної мережі організації на несанкціонований доступ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(18), 39-48. https://doi.org/10.28925/2663-4023.2022.18.3948

7. Penetration testing. IT Governance - Governance, Risk Management and Compliance for Information Technology [Електронний ресурс] Режим доступу https://www.itgovernance.co.uk/penetration-testing (28.09.2022)

Додаткова література:

1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В.Л. Бурячок, Г.М. Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.
2. Єрмошин В.В., Невойт Я.В. Аналіз і оцінка ризиків інформаційної безпеки. /Невойт Я.В., Єрмошин В.В.// Монографія. – К: ДУТ, 2015. – 124 С.
3. Богуш В.М., Довидьков О.А., Кривуца В.Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. – К.: ДУІКТ, 2010. – 454 с.