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

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
«05» ____09____ 2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «МЕТОДИ І ЗАСОБИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ»

для студентів

спеціальності	125 Кібербезпека
освітнього рівня	першого (бакалаврського)
освітньої програми	125.00.01 Безпека інформаційних і комунікаційних систем

2022 – 2023 навчальний рік

Розробник:

Бржевська Зореслава Михайлівна, доктор філософії з кібербезпеки, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:

Бржевська Зореслава Михайлівна, доктор філософії з кібербезпеки, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

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

Протокол від 01.09.2022 р. № 12

Завідувач кафедри _____ ____ Павло СКЛАДАННИЙ

(підпис)

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем)

___.___. 2022 р.

Керівник освітньої програми _____ Артем ПЛАТОНЕНКО

(підпис)

Робочу програму перевірено

___.___. 2022 р.

Заступник декана _____ Євген ІВАНІЧЕНКО

(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	обов'язкова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	4 / 120	
Курс	4	
Семестр	7	
Кількість змістових модулів з розподілом:	3	
Обсяг кредитів	4	
Обсяг годин, в тому числі:	120	
Аудиторні	42	
Модульний контроль	6	
Семестровий контроль	30	
Самостійна робота	42	
Форма семестрового контролю	екзамен	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Методи і засоби протидії кіберзлочинності» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки імені професора Володимира Бурячка на основі освітньо-професійної програми підготовки здобувачів другого (магістерського) рівня відповідно до навчального плану спеціальності 125 Кібербезпека, освітньої 125.00.01 Безпека інформаційних і комунікаційних систем.

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач першого (бакалаврського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Методи і засоби протидії кіберзлочинності» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Методи і засоби протидії кіберзлочинності» складається з трьох змістових модулів: «Нормативно-правова база та теоретичні аспекти кіберзлочинності», «Розслідування кіберзлочинів та захист даних», «Кіберпростір як метод ведення війни». Обсяг дисципліни – 120 год. (4 кредити).

Метою викладання навчальної дисципліни «Методи і засоби протидії кіберзлочинності» є формування у студентів уміння вирішувати задачі розпізнавання, розслідування кіберзлочинів та захисту конфіденційних даних, застосовувати нормативно-правові, організаційні та технічні процедури при боротьбі з кіберзлочинністю.

Завдання полягає у формуванні теоретичних знань та практичних умінь у сфері протидії кіберзлочинності та набуття **наступних фахових компетентностей**:

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

КФ 8 - Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

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.

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни студент повинен

знати:

- основні види кіберзлочинності;
- національну, міжнародну нормативно-правову базу в області кіберзлочинності;
- цифрові докази та методи аутентифікації цифрових доказів;
- ключові суб'єкти, що приймають участь в розслідуванні кіберзлочинів.

уміти:

- аналізувати проблеми технічного, правового, етичного і оперативного характеру, пов'язані з розслідуванням кіберзлочинів і попередженням кіберзлочинності;
- визначати категорії кіберзлочинності і типи кіберзлочинів, які підпадають під ці категорії;
- критично оцінювати захист прав людини в мережі Інтернет;
- порівнювати і зіставляти цифрові докази і традиційні докази для встановлення відмінностей між ними;
- роз'яснювати і критично оцінювати ресурси, які залучаються під час розслідування кіберзлочинів, і перешкоди, що виникають в ході розслідувань кіберзлочинів;
- описувати і оцінювати роль процесів управління знаннями в розслідуваннях кіберзлочинів;
- формулювати і критично оцінювати способи ідентифікації, збирання, одержання і збереження цифрових доказів.

та досягти наступних **програмних результатів навчання:**

ПРз-1 — готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки; розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем; виконувати аналіз реалізації прийнятої політики інформаційної і /або кібербезпеки.

ПРз-8 — вирішувати задачі попередження та виявлення, ідентифікації, аналізу та реагування на інциденти в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; проводити розслідування інцидентів інформаційної безпеки та/або кібербезпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної безпеки та/або кібербезпеки; забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації.

ПРз-12 - виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в інформаційно-телекомунікаційних системах; аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.

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. Основні поняття кіберзлочинності та кібербезпеки							
Тема 1. Теоретичні аспекти вивчення явища кіберзлочинності	10	2	2				6
Тема 2. Кібербезпека та центр моніторингу та управління безпекою (SOC)	12	2	2	2			6
Модульний контроль	2						
Разом	24	4	4	2			12
Змістовий модуль 2. Захист даних							
Тема 3. Принципи забезпечення безпеки мережі, мережеві атаки	14	4	2	2			6
Тема 4. Захист мережі та кінцевих пристроїв	16	4	2	4			6
Модульний контроль	2						
Разом	32	8	4	6			12
Змістовий модуль 3. Розслідування кіберзлочинів							
Тема 5. Моніторинг безпеки	12	2	2	2			6
Тема 6. Реагування на інциденти та їх аналіз	20	4	2	2			12
Модульний контроль	2						
Разом	34	6	2	2			12
Підготовка та проходження контрольних заходів	30						
Усього	**120**	**18**	**12**	**12**			**42**

5. Програма навчальної дисципліни

Змістовий модуль 1. Основні поняття кіберзлочинності та кібербезпеки

Основні питання:

- Основні поняття, пов'язані з комп'ютерним технологіям.
- Глобальні тенденції в галузі використання технологій і підключення до Інтернету.
- Визначення кіберзлочинності, проблема кіберзлочинності з наукової точки зору.
- Тенденції в області кіберзлочинності.
- Проблеми технічного, правового, етичного і оперативного характеру, пов'язані з розслідуванням кіберзлочинів і попередженням кіберзлочинності.
- Потреба в законах в області кіберзлочинності і їх роль
- Матеріальне, процесуальне і превентивне законодавство в області боротьби з кіберзлочинністю і відмінність між ними
- Національні, регіональні та міжнародні закони в області кіберзлочинності
- Захист прав людини в мережі Інтернет

Змістовий модуль 2. Захист даних

Основні питання:

- Зв'язок між безпекою та конфіденційністю.
- Закони і практичні методи, які стосуються захисту даних і повідомленнями про пошкодження систем безпеки даних, в різних країнах.
- Практичні методи контролю за дотриманням законодавства про захист даних і рекомендації ефективних способів захисту даних.
- Опис організованої кіберзлочинності і злочинних груп, які залучені в організовану кіберзлочинність.
- Структури і характеристики організованих злочинних груп, які залучені в організовану кіберзлочинність.
- Типи організованої кіберзлочинності.
- Способи застосування інформаційно-комунікаційних технологій для здійснення організованих кіберзлочинів.
- Заходи, що застосовуються для протидії організованій кіберзлочинності.

Змістовий модуль 3. Розслідування кіберзлочинів

Основні питання:

- Ключові суб'єкти, які беруть участь в розслідуваннях кіберзлочинів.
- Ресурси, які залучаються під час розслідування кіберзлочинів, і перешкоди, що виникають в ході розслідувань кіберзлочинів.
- Роль процесів управління знаннями в розслідуваннях кіберзлочинів.
- Способи ідентифікації, збирання, одержання і збереження цифрових доказів.
- Процеси, пов'язані з аналізом цифрових доказів і поданням висновків, заснованих на результатах цього аналізу.

6. Контроль навчальних досягнень

Навчальні досягнення студентів 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 студента на практичних та семінарських заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, екзамен.
- *Комп’ютерного контролю:* тести, програми-емулятори.
- *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 студентів 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.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	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	2	2	4	4	3	3
Відвідування семінарських занять	1	2	2	2	2	2	2
Відвідування практичних занять	1	1	1	2	2	2	2
Відвідування лабораторних занять	1						
Робота на семінарському занятті	10	2	20	2	20	2	20
Робота на практичному занятті	10	1	10	2	20	2	20
Лабораторна робота (в тому числі допуск, виконання, захист)	10						
Виконання завдань для самостійної роботи	5	1	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25	1	25
Виконання ІНДЗ	30						
Разом		-	54	-	78	-	77
Максимальна кількість балів: 239							
Розрахунок коефіцієнта: 239/60=3,98							

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, 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 студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1. Основні поняття кіберзлочинності та кібербезпеки		6	5
1	Національні, регіональні та міжнародні закони в області кіберзлочинності: • виконання завдань відповідно до теми; • опрацювання фахових видань.	6	5
Змістовий модуль 2. Захист даних		24	5
2	Способи ідентифікації, збирання, одержання і збереження доказів кіберзлочинів: • виконання завдань відповідно до теми; • опрацювання фахових видань.	24	5
Змістовий модуль 3. Розслідування кіберзлочинів		12	5
3	Заходи реагування на хактівізм, кібершпіонаж, кібертероризм, кібервійни, інформаційної війни, дезінформація і шахрайство на виборах: • виконання завдань відповідно до теми;	12	5

№ з/п	Назва теми	Кількість годин	Бали
	• опрацювання фахових видань.		
	Разом	72	15

Критерії оцінювання самостійної роботи студента

№ 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

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – тест, що складається 3 комплексних запитань.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі екзамену, умовою допуску до якого є отримання студентом 35 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Форма проведення екзамену – комбінована. Іспит оцінюється у 40 балів за розподілом: 20 балів – комплексний тест з дисципліни; 20 балів – виконання практико-орієнтованого завдання.

Виконання практичного завдання передбачає перевірку рівня оволодіння студентом теоретичними знаннями та практичними вміннями з навчальної дисципліни.

Оцінювання практичного завдання відбувається в межах від 0 до 20 балів, згідно критеріїв оцінювання. Бали за виконання тесту та бали за виконання практичного завдання додаються.

Орієнтовний перелік питань для семестрового контролю

1. Основні види кіберзлочинності.
2. Категорії кіберзлочинності і типи кіберзлочинів, які підпадають під ці категорії.
3. Відмінність між різними видами кіберзлочинів.
4. Способи, що використовуються для здійснення кіберзлочинів.
5. Дані і джерела даних.
6. Цифрові докази.
7. Порівняння і зіставлення цифрових доказів і традиційних доказів для встановлення відмінностей між ними.
8. Способи аутентифікації цифрових доказів.
9. Моделі процесу цифрової криміналістики.
10. Стандарти і передові практичні методи, що стосуються цифрових доказів і цифровий криміналістики.
11. Офіційні механізми міжнародного співробітництва.
12. Неофіційні механізми міжнародного співробітництва.

13. Практичні методи зберігання, забезпечення збереження даних і отримання доступу до них, які використовуються в різних країнах.
14. Проблеми, пов'язані з екстериторіальними доказами.
15. Проблема нестачі національного потенціалу для проведення розслідувань кіберзлочинів і її наслідки для міжнародного співробітництва.
16. Активи, загрози, вразливості і ризики.
17. Способи розкриття інформації про уразливість.
18. Зв'язок між кібербезпекою і зручністю використання.
19. Метод ситуаційного попередження злочинності і застосувати його для попередження і скорочення кіберзлочинності.
20. Виявлення інцидентів, реагування на них, відновлення і забезпечення готовності.
21. Визначення кіберзлочинів проти особистості.
22. Різні види кіберзлочинів проти особистості і відмінність між ними.
23. Способи використання інформаційно-комунікаційних технологій для сприяння здійсненню цих видів кіберзлочинів проти особистості.
24. Роль права в боротьбі з видами кіберзлочинами.
25. Перешкоди для вжиття заходів з попередження різних кіберзлочинів проти особистості і реагування на них.

Шкала відповідності оцінок

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

7. Навчально-методична картка дисципліни

Разом: 120 год., лекції – 18 год., практичні заняття – 12 год., лабораторні роботи – 12 год., модульний контроль – 6 год., самостійна робота – 42 год.

Модулі (назви, бали)	**Змістовий модуль 1. Основні поняття кіберзлочинності та кібербезпеки (65 бали)**		**Змістовий модуль 2. Захист даних (78 балів)**		**Змістовий модуль 3. Розслідування кіберзлочинів (77 бали)**	
Лекції (теми, бали)	Теоретичні аспекти вивчення явища кіберзлочинності (1 бал)	Кібербезпека та центр моніторингу та управління безпекою (SOC) (1 бал)	Принципи забезпечення безпеки мережі, мережеві атаки (2 бали)	Захист мережі та аналіз кінцевих пристроїв (2 бали)	Моніторинг безпеки (1 бал)	Реагування на інциденти та їх опрацювання (2 бали)
Практичні, семінарські заняття (теми, бали)		Встановлення віртуальної машини CyberOps Workstation (11 балів)	Вивчення трафіку DNS (11 балів) Атака на базу mySQL (11 балів)	Вивчення сеансів зв'язку за протоколами Telnet та SSH за допомогою програми Wireshark (11 балів)	Packet Tracer - Дослідження реалізації NetFlow (11 балів)	Інтерпретація даних HTTP та DNS для ізоляції хакера (11 балів)
Семінарські заняття (теми, бали)	Досвідчений хакер покаже нам, як це робиться (11 балів)	Кібербезпека: приклади застосування (11 балів)	Вивчення відомостей про атаку (11 балів)	Структура шкідливого програмного забезпечення (11 балів)	Соціальна інженерія (11 балів)	Обробка інцидентів (11 балів)
Самостійна робота	Самостійна робота (5 балів)		Самостійна робота (5 балів)		Самостійна робота (5 балів)	
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)		Модульна контрольна робота 2 (25 балів)		Модульна контрольна робота 3 (25 балів)	
Підсумковий контроль (вид, бали)	Екзамен (40 балів)					

8. Рекомендовані джерела

Основна (базова):

1. Бурячок В. Л. Інформаційний і кіберпростори, як нові арени воєнних дій у збройних конфліктах сучасності / В. Л. Бурячок // Спеціальна техніка у правоохоронній діяльності : матеріали V міжнар. наук.-практ. конф. (Київ, 25 листоп. 2011 р.). – К. : Нац. акад. внутр. справ України, 2012. – С. 199-201.
2. Anderson, Lorin W. and David R. Krathwohl. (2001). A Taxonomy for Learning, Teaching and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives, Complete Edition. Longman.
3. Berkeley Center for Teaching & Learning. Active Learning Strategies.
4. Bloom, Benjamin S. (1956). Taxonomy of educational objectives, Book 1: Cognitive domain. Addison-Wesley Longman.
5. Brown, Peter, Mark McDaniel, and Henry L. Roediger. (2014). Make It Stick: The Science of Successful Learning. Harvard University Press.
6. Center for Advanced Research on Language Acquisition(CARLA) (n.d.). Continuous Improvement: Objectivity and Subjectivity in Evaluation. University of Minnesota.
7. Schwartz, Michelle. (n.d.). Matching Assessments to Learning Outcomes. Ryerson University, Learning & Teaching Office.
8. Segal, Mark (2013). How To Train: A Practical Guide for Training and Working with Others.
9. Yale Poorvu Center for Teaching and Learning. Active Learning.
10. Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

Додаткова

1. Бутузов В. М. Міжнародний досвід: ініціатива правоохоронних органів Франції з протидії комп'ютерній злочинності / В. М. Бутузов // Боротьба з організованою злочинністю і корупцією (теорія і практика). – К. : МНДЦ, 2009. – № 19. – С. 240-247.
2. Чернєй В. В. Організація розслідування злочинів, пов'язаних із заволодінням коштами шляхом утручання в роботу банкоматів : метод. рек. / [В. В. Чернєй, С. С. Чернявський, О. Ю. Татаров та ін.]. – К. : Нац. акад. внутр. справ, 2013. – 88 с.
3. ЧернявськийС. С. Фінансове шахрайство : методологічні засади розслідування : моногр. / С. С. Чернявський. – К. : «Хай-Тек-Прес», 2010. – Р. 3.3.6 : Основи методики розслідування шахрайства у сфері використання комп'ютерних мереж. – С. 384-393. Х629.4 Ч-498

9. Додаткові ресурси

1. Бібліотека ресурсів E4J https://www.unodc.org/e4j/en/resdb/index.html
2. Курс Cybersecurity Operations 1.1 https://www.netacad.com/