Міністерство освіти і науки України

Харківський національний університет імені В. Н. Каразіна

Кафедра автоматизації, метрології та енергоефективних технологій

СИЛАБУС ДИСЦИПЛІНИ

НАДІЙНІСТЬ ТА КІБЕРБЕЗПЕКА СИСТЕМ КЕРУВАННЯ

рівень вищої освіти _____другий (магістерській)_____

галузь знань _____17 Електроніка, автоматизація та електронні комунікації_____
(шифр і назва)

спеціальність __174 Автоматизація, комп'ютерно-інтегровані технології та робототехніка_
(шифр і назва)

освітня програма _____Автоматизація та комп'ютерно-інтегровані технології _____
(шифр і назва)

спеціалізація _____
(шифр і назва)

вид дисципліни_____Обов'язкова _____
(обов'язкова / за вибором)

інститут _____ННІ «Українська інженерно-педагогічна академія» _____

2024 / 2025 навчальний рік

ВСТУП

Силабус навчальної дисципліни «Надійність та кібербезпека систем керування» складено відповідно до освітньо-професійної програми підготовки «Автоматизація та комп'ютерно-інтегровані технології»

_____другий (магістерській)_____
(назва рівня вищої освіти)

спеціальності _174 Автоматизація, комп'ютерно-інтегровані технології та робототехніка__

спеціалізації _____

Інформація про кафедру	Кафедра автоматизації, метрології та енергоефективних технологій Department of Automation, Metrology and Energy-efficient Technologies сайт кафедри https://kafotss.kharkov.ua/ukr/
Інформація про викладача (-ів)	Кандидат технічних наук, доцент Близниченко Олена Миколаївна посилання на профайл викладача: https://kafotss.kharkov.ua/ukr/bliznichenko_olena.html електронна пошта:o.m.blyznychenko@karazin.ua
Сторінка дисципліни в системі дистанційного навчання	https://moodle.karazin.ua/
Консультації з викладачем (-ами)	Он лайн консультації: Кандидат технічних наук, доцент Близниченко Олена Миколаївна- щовівторка 15.20 -16.40 за посиланням https://meet.google.com/ufc-wzmj-kcv

1. Опис навчальної дисципліни

1.1. Мета викладання навчальної дисципліни

Метою вивчення дисципліни «Надійність та кібербезпека систем керування» є формування у здобувачів вищої освіти ґрунтовних теоретичних знань, практичних умінь та навичок, необхідних для застосування в професійній діяльності у сфері кібербезпеки.

Дисципліна спрямована на підготовку майбутніх фахівців, здатних вирішувати складні завдання у напрямку кібербезпеки систем керування.

Вивчення навчальної дисципліни «Надійність та кібербезпека систем керування» сприяє здобуттю таких **компетентностей:**

ЗК1. Здатність проведення досліджень на відповідному рівні.

ЗК2. Здатність генерувати нові ідеї (креативність)..

СК2. Здатність проектувати та впроваджувати високонадійні системи кібербезпе-ки та їх прикладне програмне забезпечення, для реалізації функцій охорони інформації та опрацювання інформації, здійснювати захист прав інтелектуальної власності на нові проектні та інженерні рішення.

СК4. Здатність аналізувати виробничо-технологічні системи і комплекси як об’єкти автоматизації, визначати способи та стратегії їх автоматизації та цифрової трансформації.

СК7. Здатність застосовувати спеціалізоване програмне забезпечення та цифрові технології для розв’язання складних задач і проблем автоматизації та комп’ютерно-інтегрованих технологій.

1.2. Основні завдання вивчення дисципліни

1. Знання:

- правових та організаційних основ забезпечення інформаційної безпеки України та, зокрема, органів внутрішніх справ;
- основних видів загроз інформаційній безпеці та технічних каналів витоку інформації,
- методи їх виявлення та блокування;
- основних видів та можливості технічних засобів і систем захисту інформації;
- основних методів та засобів криптографічного та стенографічного захисту інформації, що циркулює у автоматизованих системах ОВС України та передаються телекомунікаційними каналами та мережами.

2. Уміння:

- планувати та організовувати свою роботу та роботу підрозділу з урахуванням вимог до захисту інформації з обмеженим доступом;
- планувати й організовувати роботи щодо створення та розвитку системи інформаційної безпеки підрозділів органів внутрішніх справ;
- організовувати роботи щодо виявлення і блокування технічних каналів витоку інформації;
- здійснювати ефективний контроль робіт із захисту інформації; здійснювати ефективний вибір комп’ютерних систем захисту;
- свідомо дотримуватися правил роботи з інформацією з обмеженим доступом та суворо виконувати вимоги до захисту інформації, що діють у системі ОВС України;
- використовувати спеціальні технічні засоби захисту інформації; використовувати програмні та апаратні засоби розмежування доступу до інформації у автоматизованих системах та антивірусні засоби захисту інформації у персональних комп’ютерах;

- використовувати комп'ютерні криптографічні, стенографічні системи захисту інформації.

3. Автономність та відповідальність:

- здатний вчитися упродовж життя і вдосконалювати з високим рівнем автономності здобуті під час навчання компетентності;

- усвідомлює соціальну значущість майбутньої професії, сформованість мотивації до здійснення професійної діяльності;

- відповідально ставиться до забезпечення охорони життя і здоров'я учнів у навально – виховному процесі та позаурочній діяльності.

1.3. Кількість кредитів а

4

1.4. Загальна кількість годин

120

1.5. Характеристика навчальної дисципліни	
Обов'язкова	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
1-й	1-й
Семестр	
2-й	2-й
Лекції	
28 год.	8 год.
Практичні, семінарські заняття	
12 год.	4 год.
Самостійна робота	
80 год.	108 год.
у тому числі індивідуальні завдання	
год.	

1.6. Заплановані результати навчання

РН02. Створювати високонадійні системи автоматизації з високим рівнем функціональної та інформаційної безпеки програмних та технічних засобів.

РН07. Аналізувати виробничо-технічні системи у певній галузі діяльності як об'єкти автоматизації і визначати стратегію їх автоматизації та цифрової трансформації.

РН08. Застосовувати сучасні математичні методи, методи теорії автоматичного керування, теорії надійності та системного аналізу для дослідження та створення систем автоматизації складними технологічними та організаційно-технічними об'єктами, кіберфізичних виробництв.

РН10. Розробляти і використовувати спеціалізоване програмне забезпечення та цифрові технології для створення систем автоматизації складними організаційно-технічними об'єктами, професійно володіти спеціальними програмними засобами.

РН11. Дотримуватись норм академічної доброчесності, знати основні правові норми щодо захисту інтелектуальної власності, комерціалізації результатів науково-дослідної, винахідницької та проектної діяльності.

2. Тематичний план навчальної дисципліни

Розділ 1. Інформаційна безпека на державному рівні*Тема 1. ПЕРЕДУМОВИ ТА ОСНОВНІ НАПРЯМКИ РОЗВИТКУ МЕНЕДЖМЕНТУ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ*

Загальні відомості. Ризики, їх класифікація. Способи порушення інформаційної безпеки. Організаційне забезпечення інформаційної безпеки.

Тема 2. ДІЯЛЬНІСТЬ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Загальні відомості. Робота міжнародних професійних об'єднань. International Telecommunication Union (ITU) – Міжнародний союз електрозв'язку. Institute of Electrical and Electronics Engineers (IEEE) – Інститут інженерів з електроніки та електротехніки. Association for Computing Machinery (ACM) – Асоціація обчислювальної техніки. World Wide Web Consortium (W3C) – Консорціум Всесвітньої Павутини. NIST – Національний інститут стандартів і технологій. International Organization for Standardization (ISO) – Міжнародна організація з стандартизації.

Тема 3. СТАНДАРТИЗАЦІЯ В СФЕРІ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Вступ. Вимоги до розроблюваних стандартів. Типи стандартів. Елементи стандартів. Огляд стандартів РГ 1.

Тема 4. РОБОТИ СПЕЦІАЛІЗОВАНИХ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ ТА ОБ'ЄДНАНЬ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Вступ. CERT Coordination Center (CERT/CC) – Координаційний центр CERT. X-Force security intelligence team – Дослідницька група X-Force. Альянси великих технологічних компаній. Smart Card Alliance (SCA) – Альянс за смарт-картками. Internet Security Alliance (ISA) – Альянс з безпеки мережі Інтернет. The International Biometric Industry Association (IBIA) – Міжнародна асоціація компаній-виробників біометричного устаткування.

Тема 5. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА РІВНІ ВЕЛИКИХ ПОСТАЧАЛЬНИКІВ ІНФОРМАЦІЙНИХ СИСТЕМ

Загальна методологія організаційного забезпечення інформаційної безпеки на рівні великих постачальників інформаційних систем. Організаційне забезпечення інформаційної безпеки на рівні окремих великих компаній.

Тема 6. ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ДЕРЖАВНОМУ РІВНІ: ПРАКТИКА США

Загальна політика США у сфері інформаційної безпеки. Структура органів державної влади, що забезпечують інформаційну безпеку в США. Федеральні програми та ініціативи, підтримувані державою.

Тема 7. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ДЕРЖАВНОМУ РІВНІ: ПРАКТИКА УКРАЇНИ

Визначення інформаційної безпеки, об'єкти, суб'єкти, основні складові. Система забезпечення інформаційної безпеки. Загрози інформаційній безпеці України у контексті діяльності Держспецзв'язку. Історія створення Держспецзв'язку. Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку). Організаційна структура Держспецзв'язку

Тема 8. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ДЕРЖАВНОМУ РІВНІ: ПРАКТИКА УКРАЇНИ (криптографічні методи захисту).

Захист державних інформаційних ресурсів в інформаційно-телекомунікаційних системах. Криптографічний захист інформації. Науково-технічна діяльність.

Тема 9. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ДЕРЖАВНОМУ РІВНІ: ПРАКТИКА УКРАЇНИ (технічні методи захисту).

Технічний захист інформації в Україні, основні аспекти. Побудова і організаційна структура системи ТЗІ в Україні. Ліцензування діяльності у галузі ТЗІ. Сертифікація засобів ТЗІ. Державна експертиза у сфері ТЗІ. Система підготовки та перепідготовки фахівців у галузі ТЗІ. Державний контроль стану КТЗІ.

Розділ 2. Інформаційна безпека на рівні підприємства

Тема 10. МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА РІВНІ ПІДПРИЄМСТВА: ОСНОВНІ НАПРЯМКИ І СТРУКТУРА ПОЛІТИКИ БЕЗПЕКИ.

Передумови розвитку менеджменту в сфері інформаційної безпеки на рівні підприємств. Загальна структура управлінської роботи щодо забезпечення інформаційної безпеки на рівні підприємства. Формування політики інформаційної безпеки на підприємстві.

Тема 11. ЗМІСТ ДЕТАЛІЗОВАНОЇ ПОЛІТИКИ БЕЗПЕКИ.

Організація внутрішньооб'єктного режиму і охорони приміщень. Фізичний захист.

Організація режиму секретності в установах і на підприємствах.

Тема 12. ДЕПАРТАМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ І РОБОТА З ПЕРСОНАЛОМ.

Департамент інформаційної безпеки. Організаційна структура та персонал департаменту інформаційної безпеки. Робота з персоналом підприємства.

Тема 13. ОРГАНІЗАЦІЯ РЕАГУВАННЯ НА НАДЗВИЧАЙНІ СИТУАЦІЇ (ІНЦИДЕНТИ).

Вступ. Виявлення атак і розпізнавання вторгнень. Локалізація та усунення наслідків. Ідентифікація нападника (або джерела розповсюдження шкідливих програм). Оцінка і подальший аналіз процесу нападу.

Тема 14. АУДИТ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ.

Аудит, види аудиту. Етапи проведення аудиту.

Тема 15. НАДАННЯ ПОСЛУГ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

Передумови розвитку ринку послуг із забезпечення інформаційної безпеки і його структура. Особливості деяких видів послуг. Інфраструктура публічних ключів.

Тема 16. НАДАННЯ ПОСЛУГ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (СТРАХУВАННЯ).

Страхування інформаційних ризиків. Основи методології страхування інформаційних ресурсів. Ринок страхових послуг.

Тема 17. МІЖНАРОДНИЙ СТАНДАРТ ISO/IEC 27001.

Розгляд міжнародного стандарту ISO/IEC 27001.

Тема 18. МІЖНАРОДНИЙ СТАНДАРТ ISO/IEC 27001. ПЕРЕЛІК ЗАХИСНИХ ЗАХОДІВ ТА ЇХ ЦІЛЕЙ.

Захисні заходи і їх цілі.

3. Структура навчальної дисципліни

Назви розділів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб.	інд.	с. р.		л	п	лаб.	інд.	с. р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Розділ 1. Інформаційна безпека на державному рівні												
Тема 1. Передумови та основні напрямки розвитку менеджменту у сфері інформаційної безпеки	7,5	2	0,5			5	6,2	1	0,2			5
Тема 2. Діяльність міжнародних організацій у сфері інформаційної безпеки	8	2	1			5	5,7	0,5	0,2			5
Тема 3. Стандартизація в сфері менеджменту інформаційної безпеки	8	2	1			5	10,7	0,5	0,2			10
Тема 4. Роботи спеціалізованих міжнародних організацій та об’єднань в галузі інформаційної безпеки	7,5	2	0,5			5	10,7	0,5	0,2			10
Тема 5. Управління інформаційною безпекою на рівні великих постачальників інформаційних систем	7,5	2	0,5			5	5,9	0,5	0,4			5
Тема 6. Організаційне забезпечення інформаційної безпеки на державному рівні: практика США	4,5	1	0,5			3	5,4	0,2	0,2			5
Тема 7. Забезпечення інформаційної безпеки на державному рівні: практика України	6,5	1	0,5			5	5,4	0,2	0,2			5
Тема 8. Забезпечення інформа-	7	1	1			5	5,4	0,2	0,2			5

ційної безпеки на державному рівні: практика України (криптографічні методи захисту)												
Тема 9. Забезпечення інформаційної безпеки на державному рівні: практика України (технічні методи захисту)	3,5	1	0,5			2	4,6	0,4	0,2			4
Разом за розділом 1	60	14	6			40	60	4	2			54
Розділ 2. Інформаційна безпека на рівні підприємства												
Тема 10. Менеджмент інформаційної безпеки на рівні підприємства: основні напрямки і структура політики безпеки	7,5	2	0,5			5	6,2	1	0,2			5
Тема 11. Зміст деталізованої політики безпеки	8	2	1			5	5,7	0,5	0,2			5
Тема 12. Департамент інформаційної безпеки і робота з персоналом	8	2	1			5	10,7	0,5	0,2			10
Тема 13. Організація реагування на надзвичайні ситуації (інциденти)	7,5	2	0,5			5	10,7	0,5	0,2			10
Тема 14. Аудит стану інформаційної безпеки на підприємстві	7,5	2	0,5			5	5,9	0,5	0,4			5
Тема 15. Надання послуг у сфері інформаційної безпеки	4,5	1	0,5			3	5,4	0,2	0,2			5
Тема 16. Надання послуг у сфері інформаційної безпеки (страхування)	6,5	1	0,5			5	5,4	0,2	0,2			5
Тема 17. Міжнародний стандарт ISO/IEC 27001	7	1	1			5	5,4	0,2	0,2			5
Тема 18. Перелік	3,5	1	0,5			2	4,6	0,4	0,2			4

захисних заходів та їх цілей												
Разом за розділом 2	60	14	6			40	60	4	2			54
Усього годин	120	28	12			80	120	8	4			108

4. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Основні поняття із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі	2
2	Етапи створення комплексної системи захисту інформації	2
3	Розробка політики безпеки інформації в ІТС	2
4	Розробка проекту комплексної системи захисту інформації	2
5	Введення комплексної системи захисту інформації в дію.	2
6	Оцінка захищеності інформації в ІТС	2
	Разом	12

5. Завдання для самостійної робота

№ з/п	Види, зміст самостійної роботи	Кількість годин
1	Системи захисту програмного забезпечення та способи їх зламу. Робота з конспектом лекцій. Робота з навчальною літературою. Підготовка до практичного заняття. Виконання розрахунково-графічної роботи. Виконання завдань для самостійної роботи на сайті дистанційної освіти.	12
2	Основні поняття операційних систем, необхідних для реалізації захисту програм. Робота з конспектом лекцій. Робота з навчальною літературою. Підготовка до практичного заняття. Виконання розрахунково-графічної роботи. Виконання завдань для самостійної роботи на сайті дистанційної освіти .	12
3	Захист програм від несанкціонованого копіювання і використання Робота з конспектом лекцій. Робота з навчальною літературою. Підготовка до практичного заняття. Виконання розрахунково-графічної роботи. Виконання завдань для самостійної роботи на сайті дистанційної освіти .	8
4	Захист програмного забезпечення від динамічного дослідження. Робота з конспектом лекцій. Робота з навчальною літературою. Підготовка до практичних занять. Виконання розрахунково-графічної роботи. Виконання завдань для самостійної роботи на сайті дистанційної освіти	18
5	Захист програм від статичного дослідження. Робота з конспектом лекцій. Робота з навчальною літературою. Підготовка до практичного заняття. Виконання розрахунково-графічної роботи. Виконання індивідуальних завдань.	18
6	Захист програм від зняття з пам’яті. Робота з конспектом лекцій. Робота з навчальною літературою. Пі-	12

	дготовка до практичного заняття. Виконання розрахунково-графічної роботи. Виконання завдань для самостійної роботи на сайті дистанційної освіти .	
	Разом	80

Теми рефератів

1. Поняття і класифікація видів та методів несанкціонованого доступу.
2. Визначення і модель зловмисника
3. Організація захисту інформації.
4. Класифікація способів захисту інформації в комп'ютерних системах
5. Фізичні методи захисту інформації
6. Законодавчі методи захисту інформації
7. Управління доступом
8. Криптографічні методи захисту інформації
9. Види умисних загроз безпеки інформації
10. Безпека оптоволоконних кабельних систем
11. Особливості слабкострумових ліній і мереж як каналів просочування інформації
12. Приховування інформації криптографічним методом

6. Індивідуальні завдання

Не передбачено навчальним планом

7. Методи навчання

Пояснювально-ілюстративний, репродуктивний, частково-пошуковий, дослідницький, проблемного викладу; словесні, наочні, практичні; аналіз, синтез, індукція, дедукція; активні методи (дискусії та дебати, метод кейсів), інтерактивні методи (інтерактивні лекції, мозкові штурми, інтерактивні симуляції), проектні методи (проектне навчання, метод проектів); методи дистанційного навчання.

8. Методи контролю

Поточний контроль – усне та письмове опитування, експрес-опитування, контрольні роботи, тестування, оцінка практичних навичок, перевірка завдань для самостійної роботи, кейс-метод, комп’ютерні симуляції.

Підсумковий контроль – іспит, курсовий проєкт.

9. Схема нарахування балів

для підсумкового семестрового контролю при проведенні семестрового екзамену

		Поточний контроль, самостійна робота, індивідуальні завдання																Екзамен	Сума
Розділ 1									Розділ 2									Разом	
T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	60	40	100
2	5	3	2	5	3	3	5	3	3	3	4	5	3	5	2	3	1			

T1, T2 ... – теми розділів

Для допуску до складання підсумкового контролю (заліку або екзамену) здобувач вищої освіти повинен набрати не менше 20 балів з навчальної дисципліни під час поточного контролю, самостійної роботи, індивідуального завдання.

Критерії оцінювання навчальних досягнень

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка	
	для чотирирівневої шкали оцінювання	для дворівневої шкали оцінювання
90 – 100	відмінно	зараховано
70-89	добре	
50-69	задовільно	
1-49	незадовільно	не зараховано

10. Рекомендована література

Основна

1. Дудатьєв А. В. Захист програмного забезпечення. Ч. 1 : навчальний посібник / Дудатьєв А. В., Каплун В. А, Семеренко В. П. – Вінниця : ВНТУ, 2005. – 140 с.

2. 1. Богуш В.М., Довидьков О.А. Теоретичні основи захищених інформаційних технологій - К.: ДУІКТ, 2010. - 508 с

3. Каплун В. А. Захист програмного забезпечення : лабораторний практикум / Каплун В. А., Дмитришин О. В., Баришев Ю. В. – Вінниця : ВНТУ, 2016. – 75 с. Штучні нейронні мережі: навчальний посібник / С. В. Ткаліченко. – Кривий Ріг, 2023. –150 с.

4. Закон України «Про захист інформації в інформаційно телекомунікаційних системах» від 31.05.2005 року, № 2594-IV, К., 2005.

5. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-2005.

6. Марущак а.І. Правові основи захисту інформації з обмеженим доступом: курс лекцій. – К.: КНТ, 2007.-208 с.

7. Бондаренко М.Ф., Черних с.П., Горбенко І.Д., Замула А.А., Ткач А.А. Методичні основи концепції і політики безпеки інформаційних технологій. Радіотехника. 2001. Вип.119.с.5-17.

8. Методологічні вказівки щодо розробки ТЗ на створення КСЗІ в АС. НД ТЗІ 3.7-001-99. з 9. Комплексна система захисту інформації (електроний ресурс, назва екрану). Режим доступу https://www.h-x.technology/ua/services/kszi implementation-ua

9. Поради (рекомендації) щодо створення КСЗІ в ІТС, які використовуються для надання послуг доступу до мережі Інтернет (електроний ресурс, назва з екрану). Режим доступу https://cip.gov.ua/ua/news/poradi-rekomendaciyi-shodo-stvorennya-kszi-v-its yaki-vikoristovuyutsya-dlya-nadannya-poslug-dostupu-do-merezhi-internet.

10. Каплун В. А. Захист програмного забезпечення : лабораторний практикум / Каплун В. А., Дмитришин О. В., Баришев Ю. В. – Вінниця : ВНТУ, 2016. – 75 с.

11. Каплун В. А., Баришев Ю. В., Дмитришин О. В.. Захист програмного забезпечення. Навчальний посібник. Частина 2. – Вінниця: ВНТУ, 2013. – 151 с.

Допоміжна

1. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT). – Київ : УкрНДНЦ, 2016.

2. Swift D. A Practical Application of SIM/SEM/SIEM Automating Threat Identification / D. Swift // SANS Institute. – 2007. – 80 p.

3. Žgela M. Security Information and Event Management – Capabilities, Challenges and Event Analysis in the Complex IT System [Electronic resource] / M. Žgela, I. Penga // Proceedings of the Central European Conference on Information and Intelligent Systems. – Varaždin, Croatia, 2019. – P. 259–266. – Access mode : http://archive.ceciis. foi.hr/app/public/conferences/2019/Proceedings/QSS/QSS4.p df.

4. Ушатов В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки / В. Ушатов, О. В. Сєвєрінов // Global Cyber Security Forum : матеріали Першого міжнародного науково-практичного форуму, 14–16 листопада 2019 р. – Харків : ХНУРЕ, 2019. – С. 104–105.

5. Pantola A. Normalization of Logs for Networked Devices in a Security Information Event Management System 343 [Electronic resource] / A. Pantola, R. Yatco, J. D. Pineda // CT Research Symposium. – De La Salle University-Manila, Philippines, 2010. – Access mode : https://www.researchgate.net/publication/286937242_Normalization_of_Logs_for_Networked_ Devices_in_a_Security_Inf ormation_Event_Management_System.

6. Incident Response Platform: The Road to Automating IR [Електронний ресурс] // Офіційний сайт компанії Cynet. – Режим доступу : https://www.cynet.com/ incident-response-services/incident-response-platform-the road-to-automating-ir/.

7. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення. НД ТЗІ 1.1-005-07.

8. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи. НД ТЗІ 3.1-001-07.

9. Типове положення про службу захисту інформації в інформаційно телекомунікаційних системах. НД ТЗІ 1.4-001.

11. Посилання на інформаційні ресурси в Інтернеті, відео-лекції, інше методичне забезпечення

1. Сторінка дистанційного навчання URL https://moodle.karazin.ua/
2. Control Systems with Neural Network URL. http://surl.li/yttvsa
3. Методи захисту програмного забезпечення від несанкціонованого копіювання [Електронний ресурс]. – Режим доступу : URL :http://www.studfiles.ru/preview/3905114 – Назва з екрану.
4. Чередниченко В. Б. Біометричні методи у системах захисту інформації / В. Б. Чередниченко, К. Е. Чередниченко // Системи обробки інформації.– 2012. – Вип. 4(1). – С. 145-148. – Режим доступу: http://nbuv.gov.ua/ UJRN/soi_2012_1_4_34.
5. OllyDbg. [Електронний ресурс]. – Режим доступу : URL : http://www. ollydbg.de/ – Назва з екрану.
7. Локазюк В.М. , Савченко Ю.Г. Надійність, контроль, діагностика і модернізація ПК – Он-лайн підручник - http://www.otk.od.ua/book/index.html
9. Журнал "CHIP" - Адрес: http://ichip.ru/
10. Український щотижневик "Мій комп'ютер" - http://mycomputer.ua/
11. https://www.netacad.com/
12. https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
13. https://zakon.rada.gov.ua/laws/show/2297-17#Text
14. https://zakon.rada.gov.ua/laws/show/3855-12#Text\
15. https://zakon.rada.gov.ua/laws/show/2657-12#Text

Зміст силабусу відповідає робочій програмі навчальної дисципліни

Завідувач кафедри АМЕТ  Геннадій КАНЮК