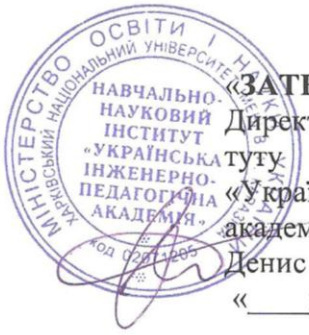
Міністерство освіти і науки України

Харківський національний університет імені В. Н. Каразіна

Кафедра Автоматизації, метрології та енергоефективних технологій



«ЗАТВЕРДЖУЮ»
Директор навчально-наукового інституту
«Українська інженерно-педагогічна академія»
Денис КОВАЛЕНКО
«____»_____2024 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Надійність та кібербезпека систем керування

(назва навчальної дисципліни)

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

2

Програму рекомендовано до затвердження вченою радою інституту ННІ «УІПА»

«_12_» ___листопада____ 2024 року, протокол №_2_

РОЗРОБНИКИ ПРОГРАМИ: Близниченко Олена Миколаївна, кандидат технічних наук, доцент, доцент кафедри АМЕТ

Програму схвалено на засіданні кафедри
_____Автоматизації, метрології та енергоефективних технологій

Протокол від «_04_» __жовтня___2024 року № _2_

Завідувач кафедри __Автоматизації, метрології та енергоефективних_технологій_____

_____ _____Канюк Г.І._____
(підпис) (прізвище та ініціали)

Програму погоджено з гарантом освітньої (професійної/наукової) програми (керівником проектної групи) _____Автоматизація та комп'ютерно-інтегровані технології

(назва освітньої програми)

Гарант освітньої (професійної/наукової) програми
(керівник проектної групи)

_____ _Василець Т.Ю._____
(підпис) (прізвище та ініціали)

Програму погоджено науково-методичною комісією
Навчально наукового інституту «Українська інженерно-педагогічна академія»
(назва факультету, для здобувачів вищої освіти якого викладається навчальна дисципліна)

Протокол від «__23__» __жовтня___2024 року № __1__

Голова науково-методичної комісії ННІ «УІПА»

_____ _____Петров С.В_____
(підпис) (прізвище та ініціали)

ВСТУП

Програма навчальної дисципліни «Надійність та кібербезпека систем керування» складена відповідно до освітньо-професійної (освітньо-наукової) програми підготовки «Автоматизація та комп'ютерно-інтегровані технології»

другий (магістерський)
(назва рівня вищої освіти)

спеціальності 174 Автоматизація, комп'ютерно-інтегровані технології та робототехніка

спеціалізації _____

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 уміннь та компетентностей щодо аналізу ризиків, проектування, розгортання та захисту високонадійних автоматизованих систем керування (АСК), з урахуванням вимог сучасної кібербезпеки, стандартів ISO/IEC, IEC 62443, NIST, та викликів індустрії 4.0.

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).

СК 2. Здатність проектувати та впроваджувати високонадійні системи кібербезпеки 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:
- принципів забезпечення кібербезпеки в АСКТП;
- типових кіберзагроз SCADA/PLC-системам та методів протидії;
- архітектури промислових мереж і вразливих точок;
- стандартів ISO/IEC 27001, IEC 62443, NIST SP 800-82;
- методів оцінювання ризиків і засобів цифрового моніторингу безпеки;
- концепції defense-in-depth, принципів сегментування, Zero Trust.

2. Уміння:
- проєктувати фрагменти архітектури захищених мереж з урахуванням SCADA/HMI;
- конфігурувати політики доступу і обліку користувачів;
- використовувати SIEM, IDS/IPS, засоби журналювання;
- виявляти та документувати кіберінциденти, проводити аналіз логів;
- розробляти політику безпеки для цифрових виробничих систем.

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;
- здатність самостійно застосовувати принципи кібербезпеки в інженерних умовах;
- здатність критично оцінювати ризики та приймати технічні рішення;
- відповідальність за забезпечення надійності промислових цифрових систем.
- здатність до самостійного прийняття технічних рішень у сфері кіберзахисту АСК.

1.3. Кількість кредитів

4

1.4. Загальна кількість годин

120

1.5. Характеристика навчальної дисципліни	
Обов'язкова / за вибором	
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 академічної доброчесності, знати правові норми захисту інтелектуальної власності.

2. Тематичний план навчальної дисципліни

Розділ 1. Система забезпечення кібербезпеки в промисловості та національній інфраструктурі

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. КІБЕРБЕЗПЕКА КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА НОРМАТИВНО-ПРАВОВА БАЗА

Основні поняття та об'єкти кібербезпеки в контексті критичної інфраструктури. Суб'єкти забезпечення інформаційної безпеки в Україні. Закон України «Про основні засади забезпечення кібербезпеки України». Нормативна база у сфері безпеки промислових систем: ISO/IEC 27001, IEC 62443, НПА КМУ, накази МОН. Координація діяльності між органами влади, установами й підприємствами.

Тема 8. КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ.

Основи криптографії в індустріальних системах. Принципи симетричного та асиметричного шифрування. Електронні підписи, PKI, SSL/TLS. Застосування криптозахисту у SCADA, PLC, IoT. Порівняння алгоритмів: AES, RSA, ECC. Вимоги до криптографічного захисту відповідно до міжнародних стандартів.

Тема 9. ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ В АСК: ІНСТРУМЕНТИ, СТАНДАРТИ, ПРАКТИКА

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. Застосування систем нечіткого висновку в задачах управління

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	8	2	1			5	5,7	0,5	0,2			5

інформаційної безпеки												
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. Кібербезпека критичної інфраструктури та нормативно-правова база	6,5	1	0,5			5	5,4	0,2	0,2			5
Тема 8. Криптографічний захист інформації в автоматизованих системах управління	7	1	1			5	5,4	0,2	0,2			5
Тема 9. Тезхнічний захист інформації в АСК: інструменти, стандарти, практика	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	8	2	1			5	10,7	0,5	0,2			10

безпеки і робота з персоналом												
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 захисних заходів та їх цілей	3,5	1	0,5			2	4,6	0,4	0,2			4
Разом за розділом 2	60	14	6			40	60	4	2			54
Усього годин	120	28	12			80	120	8	4			108

4. Теми семінарських (практичних, лабораторних) занять

№ з/п	Назва теми	Кількість годин
1	Аналіз типових загроз для SCADA-систем і побудова моделі зловмисника	2
2	Класифікація протоколів промислової автоматизації і їхні вразливості	2
3	Розробка фрагменту політики безпеки промислового об'єкта	2
4	Виявлення інцидентів на основі логів SIEM (практика з Splunk, ELK або аналогів)	2
5	Архітектура захищеної АСК: побудова сегментованої мережі з DMZ.	2
6	Аналіз кейсу кіберінциденту в АСКТП (аналіз дій і помилок)	2
	Разом	12

5. Завдання для самостійної робота

№ з/п	Види, зміст самостійної роботи	Кількість годин
1	**Аналіз стандарту IEC 62443 та його застосування в промислових АСК**. 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	**Огляд вразливостей протоколів промислової автоматизації (DNP3, Modbus, OPC-UA)**. 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	**Порівняльний аналіз інструментів SIEM, EDR, NTA для захисту АСКТП.** 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	**Розробка політики кібербезпеки для умовного SCADA-об'єкта**. 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	**Виявлення типових інцидентів у промисловій мережі. Кейсовий аналіз**. Робота з конспектом лекцій. Робота з навчальною літературою. Підготовка до практичного заняття. Виконання розрахунково-графічної роботи. Виконання індивідуальних завдань.	18
6	**Оцінка ризиків для сегментованої мережі підприємства.** 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
	Разом	80

Теми рефератів

1. Поняття і класифікація видів та методів несанкціонованого доступу.
2. Визначення і модель зловмисника.
3. Організація захисту інформації в автоматизованих системах.
4. Класифікація способів захисту інформації в комп’ютерних системах.
5. Фізичні методи захисту інформації.
6. Законодавчі методи захисту інформації.
7. Управління доступом в АСКТП.
8. Криптографічні методи захисту інформації в промислових мережах.
9. Види умисних загроз безпеці інформації в АСК.
10. Безпека оптоволоконних каналів в SCADA-системах.
11. Інформаційні витоки через слабкострумові лінії.
12. Приховування інформації криптографічним методом.
13. Стеганографічні методи приховування інформації.
14. Захист SCADA-систем: сучасні підходи.
15. Типи кібератак на PLC та інші компоненти АСКТП.
16. Протоколи безпечного обміну в АСК: аналіз вразливостей.
17. Надійність промислових мереж: оцінка і підвищення.
18. SIEM-системи: функціонал, налаштування, приклади.
19. Виявлення вторгнень у системи управління: IDS/IPS-рішення.
20. Захист PLC-контролерів: апаратні та програмні методи.

21. Кібербезпека енергетичних АСК.
22. Загрози і контрзаходи в IIoT.
23. Оцінка ризиків безпеки на виробництві: методики.
24. IEC 62443: аналіз вимог до кіберзахисту.
25. Порівняння стандартів ISO/IEC 27001 та NIST SP800-82.
26. Захист HMI-панелей в автоматизованих системах.
27. Методика тестування вразливостей у SCADA.
28. Категоризація інцидентів кібербезпеки в АСК.
29. Digital Twin у кіберзахисті.
30. Концепція Zero Trust в промислових мережах.
31. Атаки ransomware на об'єкти автоматизації: профілактика.
32. Анонімність і аудит у кіберфізичних системах.
33. Використання ШІ для виявлення аномалій в АСКТП.
34. Захист інформації в хмарних рішеннях для автоматизації.
35. Безпека бездротових каналів зв'язку у вбудованих системах.
36. Соціальна інженерія як загроза персоналу в АСКТП.
37. MITRE ATT&CK для SCADA: огляд та застосування.
38. Побудова SOC для промислових об'єктів.
39. Етичне хакерство і пентест в системах управління.
40. Юридичні аспекти відповідальності за кіберінциденти.

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.

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
3	3	3	3	3	3	3	5	4	3	3	4	5	3	3	3	3	3			

T1, T2 ... – теми розділів

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. ISO/IEC 27001:2022. Information security management systems — Requirements. – Женева : ISO, 2022. – 45 с.
2. IEC 62443-3-3:2020. System security requirements and security levels. – Женева : IEC, 2020. – 86 с.
3. NIST SP 800-82 Rev. 2. Guide to Industrial Control Systems (ICS) Security. – Gaithersburg : NIST, 2015. – 247 с.
4. Бобало Ю. Я. Інформаційна та кібербезпека : навч. посіб. / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв. – Львів : Видавництво Львівської політехніки, 2020. – 312 с.
5. Романовський О. О. Навчання кібербезпеки і кіберзахисту фахівців з управління фінансами, економікою і бізнесом : наук. вид. / О. О. Романовський, Ю. Ю. Романовська, В. Ю. Биков. – К. : ІПТО НАПН України, 2020. – 128 с.Айєрс Р. Інженерія безпеки для промислових систем : пер. з англ. / Р. Айєрс. – Харків : Фактор, 2023. – 312 с.
6. Попова І. В. Кібербезпека в епоху Індустрії 5.0: нові виклики та можливості / І. В. Попова // Економіка. Влада. Держава. – 2024. – № 3. – С. 70–77.
7. Горбаченко С. А. Роль кібербезпеки у впровадженні циркулярних економічних моделей: аналіз ризиків та можливостей / С. А. Горбаченко, Н. А. Клєвцєвич // Вісник ХНТУ. – 2024. – № 1. – С. 36–44.
8. Биков В. Ю. Кібербезпека: освіта, наука, техніка : наук. журнал. – К. : Київ. ун-т ім. Грінченка, 2020. – Т. 1, № 9. – 152 с.
9. Комп'ютерні мережі : підручник / [Азаров О. Д., Захарченко С. М.,Кадук О. В. та ін.]. − Вінниця : ВНТУ, 2020. − 378 с.Закон України «Про захист інформації в інформаційно телекомунікаційних системах» від 31.05.2005 року, № 2594-IV, К., 2005.
10. Комплексна система захисту інформації (електроний ресурс, назва екрану). Режим доступу https://www.h-x.technology/ua/services/kszi implementation-ua

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

4. 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/.

5. Документація Splunk. – [Електронний ресурс]. – Режим доступу: https://docs.splunk.com/

6. Матриця MITRE ATT&CK для ICS. – [Електронний ресурс]. – Режим доступу: https://attack.mitre.org/matrices/ics/

7. Консультації CISA для ICS. – [Електронний ресурс]. – Режим доступу: https://www.cisa.gov/ics

8. Стандарти ISA та Cybersecurity Alliance. – [Електронний ресурс]. – Режим доступу: https://www.isa.org/standards-and-publications

9. Positive Technologies. – [Електронний ресурс]. – Режим доступу: https://www.ptsecurity.com/

10. Агентство кіберінфраструктури США (CISA). – [Електронний ресурс]. – https://www.cisa.gov

11. Проєкт OWASP ICS Security. – [Електронний ресурс]. – https://owasp.org/www-project-ics-security/

12. Industrial Defender Blog. – [Електронний ресурс]. – https://industrialdefender.com/blog/

13. Агентство з кібербезпеки ЄС (ENISA). – [Електронний ресурс]. – https://www.enisa.europa.eu/

14. Посібник сертифікації IEC 62443. – [Електронний ресурс]. – https://www.isa.org/standards-and-publications/isa-iec-62443

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. STAR FORCE. Разработчики программного обеспечения [Електронний ресурс]. – Режим доступу : URL : http://www.star-force.ru/solutions/ software-developers/– Назва з екрану.

4. Методи захисту програмного забезпечення від несанкціонованого копіювання [Електронний ресурс]. – Режим доступу : URL :http://www.studfiles.ru/preview/3905114 – Назва з екрану.

5. 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.

6. 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 – Онлайн 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

Додаток 1

Додаток до робочої програми навчальної дисципліни_____
(назва дисципліни)

Дію робочої програми продовжено: на 20_____/20_____ н. р.

Заступник директора інституту ННІ «УІПА»

_____ Сергій ПЕТРОВ
(підпис) (прізвище, ініціали)

«____» _____ 20___ р.

Голова науково-методичної комісії _____ факультету

_____ _____
(підпис) (прізвище, ініціали)

«____» _____ 20___ р.