Міністерство освіти і науки України
Національний аерокосмічний університет
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№503)

ЗАТВЕРДЖУЮ

Гарант освітньої програми

_____ Д. Д. Узун
(підпис) (ініціали та прізвище)

«29» серпня 2025 р.

СИЛАБУС ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Методи та технології кібербезпеки критичних інфраструктур»
(назва навчальної дисципліни)

Галузь знань: F "Інформаційні технології"
(шифр і найменування галузі знань)

Спеціальність: F5 «Кібербезпека та захист інформації"
(код та найменування спеціальності)

Освітня програма: Безпека інформаційних і комунікаційних систем
(найменування освітньої програми)

Рівень вищої освіти:***другий (магістерський)***

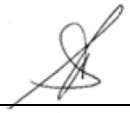
Силабус введено в дію з 01.09.2025 року

Харків – 2025р.

Розробник:  Брежнєв Є.В., проф., д.т.н
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Силабус розглянуто на засіданні кафедри комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол № 1 від « 29 » 08 2025р.

Завідувач кафедри д.т.н., професор  ВячеславХАРЧЕНКО
(науковий ступінь та вчене звання) (підпис) (ім'я таПРІЗВИЩЕ)

Погоджено з представником здобувачів освіти:


(підпис) Іван ОЛЕФІРЕНКО
(ім'я та ПРІЗВИЩЕ)

1. Загальна інформація про викладача

Брежнєв Євген Віталійович
професор кафедри комп'ютерних систем, мереж і кібербезпеки
доктор технічних наук, професор
Викладає дисципліни: «Комплексні системи захисту інформації: проектування, впровадження, супровід», «Методи дослідження комп'ютерних систем та мереж», «Методи та технології кібербезпеки критичних інфраструктур», «Технології бізнес аналітики».
Напрями наукових досліджень: застосування інформаційних технологій щодо побудови захисту складних технічних систем, методи забезпечення гарантоздатності систем що базуються на штучному інтелекті, безпека критичних інфраструктур.
Контактна інформація:
e-mail: e.brezhnev@csn.khai.edu

2. Опис навчальної дисципліни

Форма здобуття освіти	*Денна*
Семестр	2-й
Мова викладання	Українська
Тип дисципліни	*Обов'язкова*
Обсяг дисципліни: кредити ЄКТС/ кількість годин	3 кредити ЄКТС / 90 годин (48 аудиторних, з яких: лекції - 32, практичні роботи - 16)
Види навчальної діяльності	Лекції, практичні заняття.
Види контролю	Модульний контроль, семестровий контроль – іспит
Пререквізити	«Технології розроблення та забезпечення функціональної безпечності ІКС», «Методи моделювання та оптимізації безпечних КС», «Теорія та технологія розроблення безпечних та розподілених систем».

3. Мета та завдання навчальної дисципліни, переліки компетентностей та очікуваних результатів навчання

Мета: є отримання магістрами теоретичних знань і навичок з оцінювання ризиків і кібер безпеки сучасних КІ та інформаційно-керуючих систем (ІКС), використання інструментальних засобів оцінювання ризиків та кібер безпеки.

Завдання:

–є вивчення базових понять теорії ризиків та кібер безпеки критичних інфраструктур, а також методів її забезпечення..

Компетентності, які набуваються.

Інтегральна компетентність:

Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

а) загальні компетентності:

ЗК1. Здатність до адаптації та дій в новій ситуації.

ЗК2. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК3. Здатність проводити дослідження на відповідному рівні.

ЗК4. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК5. Здатність генерувати нові ідеї (креативність).

ЗК6. Здатність виявляти, ставити та вирішувати проблеми.

ЗК7. Здатність приймати обґрунтовані рішення.

Після закінчення цієї програми здобувач освіти буде здатен:

(СК1) Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

(СК2) Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.

(СК3) Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

(СК4) Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

(СК5) Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

(СК6) Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

(СК7) Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

(СК8) Здатність досліджувати, розробляти, впроваджувати супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

(СК9) Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

(СК11) Здатність аналізувати і розробляти методи і засоби оцінювання та забезпечення функційної безпечності інформаційно-керуючих систем.

(СК12) Здатність аналізувати, розробляти і впроваджувати методи і засоби розгортання безпечних хмарних та інших ІТ-інфраструктур.

Програмні результати навчання (ПРН):

ПРН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

ПРН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

ПРН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

ПРН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

ПРН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кібер. інцидентів в цілому.

ПРН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

ПРН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

ПРН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і

непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

ПРН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

ПРН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

ПРН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

ПРН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

ПРН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

ПРН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

ПРН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

ПРН24. Аналізувати та оцінювати показники функційної безпечності інформаційно-керуючих систем та обґрунтовувати рекомендації щодо її забезпечення відповідно вимогам нормативних документів.

ПРН25. Аналізувати, обґрунтовувати вибір, розробляти і впроваджувати методи і засоби розгортання безпечних хмарних та інших IT-інфраструктур.

4. Зміст навчальної дисципліни

Модуль 1. Вступ до дисципліни.

Тема 1 Критичні інфраструктури. Основні визначення, класифікація, загрози, вразливості. Основні положення “Зеленої книги з захисту критичної інфраструктури”. Смарт грид як нова генерація критичної інформаційної інфраструктури. Основні поняття захисту критичної інформаційної інфраструктури. Основні поняття ризик аналізу.

Тема Лекції 1: *«Вступ до дисципліни: методи та технології кібербезпеки критичних інфраструктур ».*

Тема Лекція 2: Основні визначення, класифікація, технології
Тема Лекція 3: Кібер безпека SCADA systems

Тема практичної роботи: Вивчення моделей аналізу аварій (кібер-інцидентів).

Тема 2 Ризик менеджмент в контексті кібер безпеки. Локальні та емерджентні ризики. Взаємодія між системами в КІ. Основні моделі кібер інцидентів та атак. Ризик аналіз функціональної безпеки інформаційно-керуючих систем в умовах невизначеності.

Тема Лекції 4: *«Ризик аналіз в контексті кібербезпеки КІ і ІКС».*
Тема Лекції 12: *«Моделі кібер інцідентів ».*

Тема практичної роботи: Порівняльній аналіз ПЗ оцінки ризиків в системах смарт грід

Тема 3 Кібер резіліенс КІ та кібер тероризм. . Основні властивості систем, що забезпечують різіліенс. Основні показники оцінювання. Функція відновлення. Кібер тероризм. Методи та інструментальні засоби оцінювання кібер безпеки. Методи оцінювання ризиків та кібер безпеки ІКС.

Тема Лекції 5: *«Резілиенс (живучість) в контексті кібер безпеки КІ».*
Тема Лекції 6: *«Метод оцінювання ризиків відмов за загальною причиною в смарт грід з урахуванням кібер ризиків».*

Тема практичної роботи: Аналіз методів та AI програмного забезпечення для оцінювання ризиків в смарт грід

Модуль 2. Методи та інструментальні засоби оцінювання кібер безпеки ІКС та КІ.

Тема 4 Нечіткі методи оцінювання кібер безпеки. Поняття нечіткої функції, нечіткої змінної. Функції належності. Нечіткі продукційні системи виводу першого роду. Нечіткі продукційні системи виводу другого роду. Лінгвістичне оцінювання кібер безпеки. Нечітка продукційна система Мамдані-Заде. Нечітка продукційна система Такаги-Сугено-Канга.

Тема Лекції 7: *«*Основні положення нечіткого оцінювання кібер безпеки КЕІ*».*

Тема практичної роботи: Застосування FuzzyLogicToolbox для аналізу кібер безпеки смарт грід

Тема 5. Методи оцінювання кібер безпеки та резіліенсу з урахуванням взаємовпливу між системами в КІ. Байесовські мережі довіри та їх застосування для задач оцінювання кібер безпеки. Матричні методи

Тема Лекції 8: *«Оцінювання взаємовпливів на резіліенс КІ».*

Тема Лекції 9: *«Оцінювання та забезпечення кібер безпеки в контексті взаємовпливів між АЄС та смарт грід».*

Тема практичної роботи: Огляд і застосування методів аналізу надійності і безпеки старт грід

Модуль 3. Методи та засоби забезпечення кібер безпеки КІ та ІКС.

Тема 6. Основні бізнес-процеси забезпечення кібер безпеки в ІТ компанії. Процесно-орієнтовані методи забезпечення кібер безпеки. Нормативно-правова база України з питань захисту КІ. Аспект кібер безпеки в законодавчій базі України.

Тема Лекції 10: «Процеси створення безпечного середовища розробки програмних додатків».

Тема Лекції 11:«Процесно-орієнтовані методи забезпечення кібербезпеки».

5. Індивідуальні завдання

№ з/п	Назва теми	Кількість годин
...	*Не передбачено*	

6. Методи навчання

Словесні (пояснення, розповідь, проблемний виклад), наочні (ілюстрування, демонстрація, презентація), практичні.

7. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді іспиту.

8. Критерії оцінювання та розподіл балів, які отримують здобувачі освіти

Таблиця 1 – Розподіл балів, які отримують здобувачі освіти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовий модуль 1,2			

Виконання і захист лабораторних робіт	0…5	3	0…15
Модульний контроль	0…25	1	0…25
Змістовий модуль 3,4			
Виконання і захист лабораторних робіт	0...5	5	0…25
Виконання і захист розрахунково-графічного завдання	0...10	1	0…10
Модульний контроль	0…25	1	0…25
Усього за семестр			**0…100**

Семестровий контроль у вигляді іспиту проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до іспиту. Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Білет для іспиту складається із двох теоретичних та одного практичного запитання, максимальна кількість балів за кожне теоретичне запитання, складає 34 балів, а за практичне – 32 балів.

Таблиця 2 – Шкали оцінювання: бальна та традиційна

Сума балів	Оцінка за традиційною шкалою
	Іспит
90-100	Відмінно
75-89	Добре
60-74	Задовільно
0-59	Незадовільно

Критерії оцінювання роботи здобувач освіти протягом семестру

Задовільно (60 – 74). Мати мінімум знань та умінь. Відпрацювати та захистити всі лабораторні роботи.

Необхідний мінімальний обсяг знань для одержання задовільної оцінки:

- знати основні положення “Зеленої книги з захисту критичної інфраструктури”.
- знати основні поняття захисту критичної інформаційної інфраструктури, ризик аналізу.
- знати основні процесно-орієнтовані методи забезпечення кібер безпеки.
- Знати основні методи забезпечення інформаційної безпеки підприємства.

Необхідний обсяг вмінь для одержання задовільної оцінки:

- вміти проводити аналіз аварій (кібер інцидентів) із застосуванням моделей.
- вміти застосовувати програмне забезпечення Cafta & Netica для інтегрування методів оцінювання надійності та безпеки смарт грід (ІКС)

Вміти самостійно визначати основні елементи захисту критичної інформаційної інфраструктури та її ризик аналізу. Вміти аналізувати аварій (кібер інциденти) в смарт грід.

Добре (75 – 89). Твердо знать мінімум знань, виконати не менше 90% завдань лабораторних занять.

Окрім знань, необхідних для отримання оцінки задовільно, для отримання оцінки добре необхідно:

- знати основні властивості систем, що забезпечують різіліенс. Вміти формулювати та визначати показники різіліенсу. Застосовувати методи та інструментальні засоби оцінювання кібер безпеки, а також методи оцінювання ризиків та кібер безпеки ІКС. Вміти проектувати бізнес-процеси забезпечення кібер безпеки в компанії.

Відмінно (90 – 100). Повно знати основний та додатковий матеріал. Орієнтуватися у підручниках та посібниках. Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти застосовувати їх. Безпомилково виконувати та захищати всі роботи в обумовлений викладачем строк з докладним обґрунтуванням рішень та заходів, які запропоновано у роботах.

9. Політика навчального курсу

Відвідування занять. Регуляція пропусків. Характер курсу передбачає необхідність відвідування занять. Здобувачі освіти, які за певних обставин не можуть відвідувати заняття регулярно, повинні протягом тижня узгодити із викладачем графік індивідуального відпрацювання пропущених занять. Окремі пропущені заняття мають бути відпрацьовані на найближчій консультації протягом тижня після їх пропуску. Відпрацювання занять здійснюється усно у формі співбесіди за питаннями, визначеними планом заняття. В окремих випадках дозволяється письмове відпрацювання пропущених занять шляхом виконання індивідуального письмового завдання.

Дотримання вимог академічної доброчесності здобувачами освіти під час вивчення навчальної дисципліни. Під час вивчення навчальної дисципліни здобувані освіти мають дотримуватися загальноприйнятих морально-етичних норм і правил поведінки, вимог академічної доброчесності, передбачених Положенням про академічну доброчесність Національного аерокосмічного університету«Харківський авіаційний інститут» (https://khai.edu/assets/files/polozhennya/polozhennya-pro-akademichnu-dobrochesnist.pdf). Очікується, що роботи здобувачів освіти будуть їх оригінальними дослідженнями або міркуваннями. Списування, втручання в роботу інших здобувачів освіти становлять, але не обмежують, приклади можливої академічної недоброчестності. Виявлення ознак академічної недоброчесності в письмовій роботі здобувача освіти є підставою для її незарахування викладачем незалежно від масштабів плагіату чи обману.

Вирішення конфліктів. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, а також правила етичної поведінки регламентуються Кодексом етичної поведінки в Національному аерокосмічному університеті «Харківський авіаційний інститут» (https://khai.edu/ua/university/normativna-baza/ustanovchi-dokumenti/kodeks-etichnoi-povedinki/).

10. Методичне забезпечення

Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=1617

11. Рекомендована література

Базова

1. V. Kharchenko, V. Sklyar, E. Brezhniev, 2013, Safety of information and control systems. Models, techniques and technologies – Palmarium Academic Publishing, pp. 528.
2. R. Bloomfield, K. Netkachova, R. Stroud, 2013, "Security-Informed Safety: If It's Not Secure, It's Not Safe", Software Engineering for Resilient Systems Lecture Notes in Computer Science, Volume 8166, Springer Berlin Heidelberg, pp. 17-32.
3. Yastrebenetsky, M., Kharchenko, V., 2014, "Nuclear power plant instrumentation and control systems for safety and security", IGI Global, pp. 470.
4. M. Yastrebenetsky, V. Kharchenko (Edits), "*Nuclear Power Plant Instrumentation and Control Systems for Safety and Security*", A volume in the Advances in Environmental Engineering and Green Technologies (AEEGT) Book Series, Hershey, Pennsylvania, United States of America, IGI Global, 2014, 470 p.
5. Huffmire, C. Irvine, T.D. Nguyen, "*Handbook of FPGA Design Security*", Springer, 2010, 177 p.
6. V. Kharchenko, A. Kovalenko, V. Sklyar, O. Siora, "Security Assessment of FPGA-based Safety-Critical Systems: US NRC Requirements Context", Proceedings of the International Conference on Information and Digital Technologies (IDT 2015), Žilina, Slovakia, July 7-9, 2015, pp. 117-123.
7. Momoh, J. A, "Fundamentals of analysis and computation for the Smart Grid," Power and Energy Society General Meeting, 2010 IEEE , vol., no., pp.1-5, 25-29 July 2010.
8. Arnold, G. W, "Challenges and Opportunities in Smart Grid: A Position Article," Proceedings of the IEEE, vol.99, no.6, pp.922-927, June 2011.
9. ISO/IEC 27000:2009 Information technology — Security techniques — Information security management systems — Overview and vocabulary (IDT).

10. NIST SP800-30 Risk Management Guide for Information Technology Systems Text]. – National Institute of Standards and Technology 2002 – 95 p.
11. Byres, E. J., Franz, M. and Miller, D., “The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems”, International Infrastructure Survivability Workshop (IISW '04), IEEE, Lisbon, Portugal, December 4, 2004.
12. Scambray, J. and McClure, S., “Hacking Exposed Windows 2000: Network Security Secrets and Solutions,” McGraw_Hill, 2001.
13. B. Utne, P. Hokstad, G. Kjolle, J. Vatn, I.A. Tendel, D. Bertelsen, H. Fridheim, J. Rustrum, Risk and Vulnerability Analysis of Critical Infrastructures - The DECRIS approach.
14. U.S. Department of Homeland Security. NIPP 2013: Partnering for Critical Infrastructure Security and Resilience, Washington, DC, 2013.
15. R. Belohlavek, V. Vychodil, Attribute implications in a fuzzy setting, in: B. Ganter, L. Kwuida (Eds.), Lecture Notes in Artificial Intelligence, vol. 3874, Springer-Verlag, Heidelberg, 2015.

Допоміжна

1. Rinaldi, J.Peerenboom Identifying, Understanding, and Analyzing Critical Infrastructure Dependencies /IEEE Control Systems Magazine, Vol. 21 - Dec. 2001 - pp. 11-25.
2. Singer, D. 1990. A fuzzy set approach to fault tree and reliability analysis. FuzzySets and Systems, 34, 2: 145-55.
3. Wayne C. Turner, Steve Doty Energy management handbook, Sixth edition, Fairmont Press, Inc, 2006, 389 p.
4. Cai, K.Y., Wen, C.Y., and Zhang, M.L. 1991. Fuzzy variables as a basis for a theory of fuzzy reliability in the possibility context. Fuzzy Sets and Systems, 42, 2: 145-172.
5. Cai, K.Y., Wen, C.Y., and Zhang, M.L. 1991. Posbist reliability behavior of typical systems with two types of failures. Fuzzy Sets and Systems, 43, 1:17-32.
6. Cai, K.Y., Wen, C.Y., and Zhang, M.L. 1993. Fuzzy states as a basis for a theory of fuzzy reliability. Microelectronic Reliability, 33, 1: 2253-2263.
7. MIL-STD-1629A, Procedures for Performing a Failure Mode, Effects, and Criticality Analysis, 24 Nov. 1980.
8. Pederson, P., Dudenhoeffer, D., Hartley, S. & Perman, M. 2006. Critical Infrastructre Interdependency modelling: A survey of U.S and international research. Report prepared by the Idaho National Laboratory.

12. Інформаційні ресурси

1. The MathWorks. Fuzzy Logic Toolbox. [Ел. ресурс]. URL: http://www.mathworks.com/products/fuzzylogic/
2. Actionable Vendor Risk Management [Ел. ресурс]. URL: https://www.cyberriskanalytics.com/

3. Risk and Compliance Management Platform [Ел. ресурс]. URL: https://www.riskwatch.com/
4. Risk Management Standards [Ел. ресурс]. URL: https://www.enisa.europa.eu/publications/risk-management-standards
5. NIS2 Technical Implementation Guidance [Ел. ресурс]. URL: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance
6. Cyber Insurance - Models and methods and the use of AI [Ел. ресурс]. URL: https://www.enisa.europa.eu/publications/cyber-insurance-models-and-methods-and-the-use-of-ai
7. NIST Cybersecurity Framework [Ел. ресурс]. URL: http://www.nist.gov/cyberframework/upload/cybersecurity-framework.
8. NISTIR 7628 Guidelines for Smart Grid Cyber Security[Ел. ресурс]. URL: https://www.nist.gov/smartgrid/upload/nistir-7628.
9. Quantitative Risk Reduction Estimation Tool for Control Systems – Suggested Approach and Research Needs [Ел. ресурс]. URL: https://inldigitallibrary.inl.gov/sites/STI/STI/3394954.pdf