Національний аерокосмічний університет
«Харківський авіаційний інститут»

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

ЗАТВЕРДЖУЮ

Гарант освітньої програми


Олег ІЛЛЯШЕНКО
(підпис) (ім'я та ПРІЗВИЩЕ)

« 29 » серпня 2025 р.

СИЛАБУС ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Кваліфікаційна робота бакалавра
(назва навчальної дисципліни)

Галузь знань: 12 «Інформаційні технології»
(шифр і найменування галузі знань)

Спеціальність: 125 Кібербезпека та захист інформації
(код і найменування спеціальності)

Освітньо-професійна програма: «Кібербезпека та захист інформації»
(найменування освітньої програми)

Рівень вищої освіти: **перший (бакалаврський)**

Силабус введено в дію з 01.09.2025

Харків – 2025 р.

Розробник: Ілляшенко О.О., доцент, к.т.н., доцент
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

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

Протокол № 1 від « 29 » серпня 2025 р.

Завідувач кафедри д.т.н., професор Вячеслав ХАРЧЕНКО
(науковий ступінь і вчене звання) (підпис) (ім'я та ПРІЗВИЩЕ)

Погоджено з представником здобувачів освіти:

(підпис) Ілля МІЦИК
(ім'я та ПРІЗВИЩЕ)

1. Загальна інформація про викладача

ПІБ: Ілляшенко Олег Олександрович

Посада: доцент кафедри комп'ютерних систем, мереж і кібербезпеки

Науковий ступінь: кандидат технічних наук

Вчене звання: доцент

Перелік дисциплін, які викладає:

Стандартизація і сертифікація систем кібербезпеки

Напрями наукових досліджень:

Розвідка кіберзагроз/запобігання кібербазгрозам; Безпека вбудованих систем критичного застосування; Оцінка, забезпечення та стандартизація промислової автоматизації та систем управління

Контактна інформація:

o.illiashenko@khai.edu

2. Опис навчальної дисципліни

Форма здобуття освіти	Денна
Семестр	8
Мова викладання	Українська, англійська
Тип дисципліни	Обов'язкова
Обсяг дисципліни: кредити ЄКТС/ кількість годин	9 кредитів ЄКТС / 270 годин (0 аудиторних, з яких: СРЗ – 270)
Види навчальної діяльності	Самостійна робота здобувача
Види контролю	Нормоконтроль, перевірка на наявність плагіату, публічний захист кваліфікаційної роботи
Пререквізити	Дисципліна є обов'язковим компонентом освітньої програми і базується на усіх знаннях, отриманих під час вивчення дисциплін у циклі загальної і професійної підготовки, передбачених навчальним планом спеціальності

3. Мета та завдання навчальної дисципліни

Мета навчання: визначення рівня підготовленості здобувача першого рівня вищої освіти до розв'язання комплексу сучасних наукових і прикладних завдань в області сучасних інформаційних технологій, зокрема, кібербезпеки та безпеки інформаційних і комунікаційних систем, на основі застосування системи теоретичних знань і практичних навичок, отриманих у процесі всього періоду навчання відповідно до вимог стандарту вищої освіти.

Завдання: систематизація, закріплення і розширення теоретичних знань, отриманих у процесі навчання за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем», їх практичне використання при вирішенні конкретних наукових, прикладних, інженерних і виробничих питань у галузі професійної діяльності 12 «Інформаційні технології»; розвиток навичок самостійної роботи, оволодіння методиками досліджень і експериментування, моделювання, використання сучасних інформаційних технологій у процесі розв'язання задач з проєктування, оцінювання та забезбечення захисту систем кібербезпеки та захисту інформації, які передбачені завданням на дипломне проектування; визначення відповідності рівня підготовки здобувача вищої освіти першого рівня вимогам характеристик фахівця освітнього ступеню, його готовності та спроможності до самостійної роботи в умовах ринкової економіки, сучасного виробництва, прогресу науки, техніки і культури.

Компетентності, які набуваються:

***Інтегральна компетентність*:** Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми під час професійної діяльності, або навчання, що передбачає застосування теорій, моделей, засобів розроблення, оцінювання, та забезпечення кібербезппеки комп’ютерних обчислювальних систем, і характеризується комплексністю та невизначеністю умов.

Занальні компетентності.

– КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

– КЗ 2. Знання та розуміння предметної області та розуміння професії.

– КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

– КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

– КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

– КЗ 6. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні;

– КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та

закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

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

– КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

– КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

– КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

– КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

– КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.

– КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

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

– КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпеки.

– КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

– КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

– 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.

4. Програмні результати навчання. В результаті вивчення дисципліни студенти мають досягти такі програмні результати навчання:

– ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;

– ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та

практичних проблем у професійній діяльності, оцінювати їхню ефективність;

– ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

– ПРН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

– ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;

– ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

– ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;

– ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;

– ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;

– ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;

– ПРН 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;

– ПРН 12. Розробляти моделі загроз та порушника;

– ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;

– ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;

– ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;

– ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;

– ПРН 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;

– ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;

– ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;

– ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;

– ПРН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматзованих) системах;

– ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;

– ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

– ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);

– ПНР 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;

– ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;

– ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;

– ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки;

– ПРН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;

– ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;

– ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;

– ПРН 32. Вирішувати задачі управління процесами відновлення

штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;

– ПРН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;

– ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;

– ПРН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;

– ПРН 36. Виявляти небезпечні сигнали технічних засобів;

– ПРН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;

– ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;

– ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;

– ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;

– ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;

– ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;

– ПРН 44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;

– ПРН 45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;

– ПРН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;

– ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;

– ПРН 48. Виконувати впровадження та підтримку систем виявлення

вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;

– ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;

– ПРН 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);

– ПРН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;

– ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;

– ПРН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз

– ПРН 54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

4. Зміст навчальної дисципліни

Модуль 1.
Змістовний модуль 1. Підготовка дипломної роботи та захист

Тема 1. Видача завдання. Постановка задачі.

Обґрунтування напряму роботи та постановка задачі подальшого дослідження.

Тема 2. Аналіз предметної області.

Систематизація та аналіз літературних джерел з питань, що вивчаються під час підготовки кваліфікаційної роботи, з урахуванням кращих структурних, методичних, алгоритмічних, програмних, технологічних та виробничих досягнень, наявних на момент підгтовки. Ґрунтовне та системне викладення сучасного стану питань та задач, що розв’язуються в процесі підготовки кваліфікаційної роботи. Робота з англомовними джерелами.

Тема 3. Аналіз існуючих рішень.

Систематизація та аналіз існуючих методологічних, технологічних, програмних, програмно-апаратних рішень з питань, що вивчаються під час підготовки кваліфікаційної роботи. Ґрунтовне та системне порівняння властивостей та перспектив розвитку об’єктів, процесів, та рішень, що аналізуються. Обґрунтування основі проведеного аналізу рішення, що пропонується у кваліфікаційній роботі.

Тема 4. Розроблення та/чи аналіз запропонованого рішення.

Мета та опис програми та послідовності розроблення та/чи аналізу запропонованого методологічного, технологічного, програмного, програмно-апаратного рішення, проведення експериментів, їх суть, оцінки точності та вірогідності отриманих даних. Співставлення теоретичних та експериментальних даних, результати розробки безпечних інформаційних і комунікаційних систем. Технологічне забезпечення процесу створення безпечних інформаційних і комунікаційних систем.

Тема 5. Нормативно-правове забезпечення

Аналіз національних та міжнародних нормативно-правових документів та документів з технічного регулювання запропонованого в кваліфікаційній роботі рішення.

Тема 6. Розроблення пояснювальної записки.

Оформлення пояснювальної записки відповідно до правил оформлення навчальних і науково-дослідних документів та вимог ДСТУ 3008:2015. Перевірка пояснювальної записки на предмет порушення академічної доброчесності.

Тема 7. Розроблення презентації та публічний захист.

Розроблення презентації. Підготовка доповіді. Публічний захист кваліфікаційної роботи бакалавра.

5. Індивідуальні завдання

Тема кваліфікаційної роботи бакалавра має відповідати предметній області, для якої був виконаний звіт з виробничої практики. Теми кваліфікаційних робіт бакалаврів можуть бути запропоновані керівником виробничої практики, керівником кваліфікаційної роботи або сформульовані самими студентами. Індивідуальне завдання на кваліфікаційну роботу погоджується з керівником кваліфікаційної роботи. Ці теми закріплюються за здобувачами, розглядаються, та затверджуються на засіданні кафедри на початку четвертого курсу навчання.

6. Методи навчання

Проведення консультацій, а також самостійна робота студентів із використання відповідних матеріалів (пп.11 – 12).

7. Методи контролю

Семестровий контроль проводиться у формі нормоконтролю, перевірки на наявність плагіату та публічного захисту кваліфікаційної роботи бакалавра.

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

Таблиця 8.1 – Розподіл балів, які отримують здобувачі освіти

Складові навчальної роботи	Сумарна кількість балів
Тема 1. Видача завдання. Постановка задачі	0…5
Тема 2. Аналіз предметної області	0…10
Тема 3. Аналіз існуючих рішень	0…15
Тема 4. Розроблення та/чи аналіз запропонованого рішення	0…40
Тема 7. Розроблення презентації	0…10
Нормоконтроль	0…5
Перевірка на плагіат	0…5
Публічний захист	0…10
Усього	0…100

Таблиця 8.2 – Шкали оцінювання: бальна і традиційна

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

8.1. Якісні критерії оцінювання

Кваліфікаційна робота має бути виконана у відповідності до закріпленої теми, оформлена згідно затверджених вимог до дипломних робіт і своєчасно представлена до захисту. Автор кваліфікаційної роботи повинен продемонструвати: вміння логічно та аргументовано викладати матеріал, коректно використовувати статистичні, математичні та інші методи, проводити власні дослідження; володіння навичками узагальнення, формулювання висновків; вміння працювати з інформаційними джерелами; вміння ініціювати та обґрунтовувати інноваційні підходи до вирішення проблеми, що досліджується.

8.2. Критерії оцінювання роботи здобувача протягом семестру

Критеріями оцінювання дипломної роботи є:

- чіткість, повнота та послідовність розкриття кожного питання і теми роботи в цілому в теоретичній і практичний площині;
- правильне оформлення роботи відповідно до затверджених стандартів;
- відсутність орфографічних і синтаксичних помилок;
- наявність додатків з публікацією та апробацією результатів.

Оцінка визначається як сума балів за суть, оформлення і представлення на захисті роботи згідно із наступною орієнтовною шкалою:

1. **Задовільно** (60-74). Показати мінімум знань та умінь. Уміти обґрунтувати тему (актуальність, практичну значимість, сформулювати мету і завдання роботи); продемонструвати результати огляду підходів, аналізу існуючих рішень; продемонструвати результати дослідницької частини (виконання поставлених задач, отримані результати під наглядом керівника, проєктування, розроблення тощо); уміти працювати над дипломною роботою впродовж семестру під наглядом дипломного керівника.

2. **Добре** (75-89). Твердо знати необхідний обсяг знань для одержання позитивної оцінки, продемонструвати результати огляду підходів, аналізу існуючих рішень, та зроботи постановку задачі; продемонструвати результати дослідницької частини (виконання поставлених задач, самостійно отримані результати, проєктування, розроблення тощо); уміти самостійно та ритмічно працювати над дипломною роботою впродовж семестру.

3. **Відмінно** (90-100). Відмінно знати та демонструвати під час захисту дипломної роботи необхідний обсяг знань для одержання позитивної оцінки. Уміння формулювати напрями подальших досліджень, запропоновувати покращення. Досконально знати всі теми та уміти їх застосовувати. Уміти самостійно та ритмічно працювати над дипломною роботою впродовж семестру.

9. Політика навчального курсу

Дотримання вимог академічної доброчесності здобувачами освіти під час вивчення навчальної дисципліни. Під час вивчення навчальної дисципліни здобувачі 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. Відсутність посилань на використані джерела, фабрикування джерел, 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

Навчально-методичний комплекс дісциплини розміщений у системі управління курсами кафедри комп'ютерних систем, мереж та кібербезпеки.

Система управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки [Ел. ресурс]. URL: https://elearn.csn.khai.edu

11. Рекомендована література

1) Базова

1. Корягін М.В., Чік М.Ю. Основи наукових досліджень: навч. посібник; 2-ге вид., доп. і перероб. К: Центр навч. і практ. літ-ри, 2019. – 492 с.
2. Правила оформлення навчальних і науково-дослідних документів: навч. посіб. / Ю. А. Воробйов, Ю. О. Сисоєв. 4-те вид. [Ел. ресурс]. URL: http://library.khai.edu/library/fulltexts/metod/Vorobjov_Pravila.pdf
3. Gorbenko, A., Kharchenko, V., Tarasyuk, O., Furmanov, A.: F(I)MEA-technique of Web Services Analysis and Dependability Ensuring. Lecture Notes in Computer Science, vol. 4157, pp. 153-167 (2006)
4. Babeshko, E., Kharchenko, V., Gorbenko, A.: Applying F(I)MEA-technique for SCADA-based industrial control systems dependability assess- ment and ensuring. In: Third International Conference on Dependability of Computer Systems DEPCOS- RELCOMEX, pp. 309-315 (2008)
5. Bloomfield, R., Netkachova. K., Stroud. R.: Bloomfield, R. Security-Informed Safety: If It's Not Secure, It's Not Safe. In: Software engineering for resilient systems lecture notes in computer science volume 8166, pp. 17-32, Springer Berlin Heidelberg (2013)
6. Ілляшенко, О.О.: Оцінювання інформаційної безпеки систем на програмовній логіці з використанням кейсів: таксономія, нотація, концепція. Наука і Техніка Повітряних Сил Збройних Сил України, № 2(31), с. 97-103 (2018)
7. Illiashenko, O., Potii, O., Komin, D.: Advanced security assurance case based on ISO/IEC 15408. In: Theory and Engineering of Complex Systems зфtand Dependability, Proceedings of the Tenth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX, Advances in Intelligent Systems and Computing, pp. 391-401. Poland, Brunów (2015) (SCOPUS)
8. О. Ілляшенко, Методи і засоби забезпечення виконання вимог до кібербезпеки систем на програмовній логіці: моногр. / за ред. В. С. Харченка. – Міністерство освіти і науки України, Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», 2019. – 195 с.

2) Допоміжна

1) The Adelard Safety Case Editor – ASCE. In: Adelard. https://www.adelard.com/asce/

2) Assurance and Safety Case Environment (ASCE) help manual. In: Adelard, https://www.adelard.com/media/zvrdth3l/mk95v12_asce_51.pdf

3) SESAMO project. Security and safety modelling. http://sesamo-project.eu.

4) ECHO project. European network of Cybersecurity centres and competence Hub for innovation and Operations. https://echonetwork.eu/

5) SYNAPSE project. An Integrated Cyber Security Risk & Resilience Management Platform, With Holistic Situational Awareness, Incident Response & Preparedness Capabilities https://www.synapse-project.eu/

6) K. Hovhannisyan, P. Bogacki, C. A. Colabuono, D. Lofù, M. V. Marabello and B. Eugene Maxwell, "Towards a Healthcare Cybersecurity Certification Scheme," 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 2021, pp. 1-9, doi: 10.1109/CyberSA52016.2021.9478255.

7) Державна служба спеціального зв'язку та захисту інформації України ДСТЗІ. Засоби ТЗІ, які мають експертний висновок про відповідність до вимог технічного захисту інформації [Ел. ресурс]. URL: https://cip.gov.ua/ua/news/zasobi-tzi-yaki-mayut-ekspertnii-visnovok-pro-vidpovidnist-do-vimog-tekhnichnogo-zakhistu-informaciyi

3) Закони України

1. Закон України «Про державну таємницю» від 21 січня 1994, Документ 3855-XII, чинний, поточна редакція — Редакція від 05.08.2018, підстава - 2509-VIII, https://zakon.rada.gov.ua/laws/show/3855-12

2. Закон України «Про інформацію», від 02.10.92, 1992, Документ 2657-XII, чинний, поточна редакція — Редакція від 16.07.2019, підстава - 2704-VIII, https://zakon.rada.gov.ua/laws/main/2657-12

3. Закон України «Про науково-технічну інформацію» від 25.06.1993, Документ 3322-XII, чинний, поточна редакція — Редакція від 19.04.2014, https://zakon.rada.gov.ua/laws/main/3322-12

4. Закон України «Про внесення змін до Закону України "Про захист інформації в автоматизованих системах», Документ 2594-IV, чинний, поточна редакція — Прийняття від 31.05.2005, https://zakon.rada.gov.ua/laws/main/2594-15

5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», 1994, Документ 80/94-ВР, чинний, поточна редакція — Редакція від 19.04.2014, https://zakon.rada.gov.ua/laws/main/80/94-%D0%B2%D1%80

6. Закон України «Про Національну систему конфіденційного зв'язку», 2002, Документ 2919-III, чинний, поточна редакція — Редакція від 19.04.2014, https://zakon.rada.gov.ua/laws/main/2919-14

7. Закон України «Про національну безпеку України» Документ 2469-VIII, чинний, поточна редакція — Прийняття від 21.06.2018, https://zakon.rada.gov.ua/laws/main/2469-19

8. Закон України «Про основні засади забезпечення кібербезпеки України», 2017, Документ 2163-VIII, чинний, поточна редакція — Редакція від 08.07.2018, https://zakon.rada.gov.ua/laws/main/2163-19

9. Указ Президента України «Про заходи щодо захисту інформаційних ресурсів держави» від 10.04.2000, Документ 582/2000, поточна редакція — Прийняття від 10.04.2000, https://zakon.rada.gov.ua/laws/show/582/2000

10. Указ президента україни «Про Положення про технічний захист інформації в Україні», Документ 1229/99, поточна редакція — Редакція від 04.05.2008, https://zakon.rada.gov.ua/laws/show/1229/99

11. Постанова Кабінету Міністрів України від 8 жовтня 1997 р. N 1126 «Про затвердження Концепції технічного захисту інформації в Україні». Документ 1126-97-п, поточна редакція — Редакція від 13.10.2011, підстава - 938-2011-п. https://zakon.rada.gov.ua/laws/main/1126-97-%D0%BF

4) Укази Президента України.

1. №1556 от 07.11.2005 "Про додержання прав людини під час проведення оперативно-технічних заходів".

2. № 891 від 24.09.2001 року "Про деякі заходи щодо захисту державних ін формаційних ресурсів у мережах передачі даних".

3. №582 від 10.04 2000 року "Про заходи щодо захисту інформаційних ресурсів держави"

4. № 1229 від 27.09.1999 року "Про Положення про технічний захист ін формації в Україні".

5. № 505 від 22.05. 1998 року "Про Положення про порядок здійснення криптографічного захисту інформації в Україні".

5) Постанови КМУ

1. Постанова КМ від 29 березня 2006 р. N 373 " Про затвердження Правил за-безпечення захисту інформації в інформаційних, телекомунікаційних та ін формаційно-телекомунікаційних системах"

2. КМ України Постанова КМ, від 03.08.2005 р. N 688 "Про затвердження Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління"

6. КМ України Постанова КМ, від 28.10.2004 р. N 1452 "Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності"

3. КМ України Постанова КМ, від 28.10.2004 р. N 1453 "Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади"

4. КМ України Постанова КМ, від 28.10.2004 р. N 1454 "Про затвердження Порядку обов'язкової передачі документованої інформації"

5. КМ України Постанова КМ, від 16.11.2002 р. N 1772 "Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах"

6. КМ України Постанова КМ, від 04.02. 1998, N 121 "Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних"

7. КМ України Постанова КМ, від 08.10.1997, № 1126 "Про затвердження Концепції технічного захисту інформації в Україні"

8. КМ України Постанова КМ, від 16.02.1997, №180 "Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах".

6) Стандарти та технічне регулювання

1. ДСТУ 3008:2015. Інформація та документація. Звіти у сфері науки і техніки: Структура і правила оформлювання. – К.: ДП «УкрНДНЦ», 2016. – 26 с.

2. ДСТУ 8302:2015. Інформація та документація. Бібліографічне посилання: Загальні положення та правила складання. – К.: ДП «УкрНДНЦ», 2016. – 16 с.

3. Державний стандарт України Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96

4. Державний стандарт України Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96

5. Державний стандарт України Захист інформації. Технічний захист інформації. Терміни та визначення. ДСТУ 3396.2-97

6. Нормативні документи системи ТЗІ https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi

7. Міжнародні стандарти Режим доступу: https://www.iso.org/ru/home.html

8. Європейські стандарти. Режим доступу: https://www.etsi.org/standards#Security

9. Національні нормативні документи: https://cip.gov.ua/ua/docs

10. Державний стандарт України Обробляння інформації. Символи та угоди щодо документації стосовно даних, програм та системних блок-схем, схем мережевих програм та схем системних ресурсів. ДСТУ ISO 5807:2016

11. ДСТУ EN 61508-1:2019 Функційна безпечність електричних, електронних, програмованих електронних систем, пов’язаних із безпекою. Частина 1. Загальні вимоги (EN 61508-1:2010, IDT; IEC 61508-1:2010, IDT)

12. ДСТУ ISO/IEC 15408-1:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель (ISO/IEC 15408-1:2009, IDT)

13. ДСТУ ISO/IEC 15408-2:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги (ISO/IEC 15408-2:2008, IDT)
14. ДСТУ ISO/IEC 15408-3:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 3. Вимоги до гарантії безпеки (ISO/IEC 15408-3:2008, IDT)
15. ДСТУ ISO/IEC 18045:2015 Інформаційні технології. Методи захисту. Методологія оцінювання безпеки IT (ISO/IEC 18045:2008, IDT)
16. ISO/IEC 15443-1:2012: International Organization for Standardization. International Electrotechnical Commission. Information technology – Security techniques.
17. ISO/IEC TR 15443-2:2012: International Organization for Standardization. International Electrotechnical Commission. Information technology - Security techniques - A framework for IT security assurance – Part 2: Assurance methods.
18. ISO/IEC TR 15443-3:2012: International Organization for Standardization. International Electrotechnical Commission. Information technology - Security techniques - A framework for IT security assurance - Part 3: Analysis of assurance methods.
19. ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT).
20. NIST SP 800-50 - Створення програми підвищення обізнаності в області безпеки IT https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf
21. NIST SP 800-40 - Керівництво по технологіям управління уразливостями https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf
22. NIST 800-53 – Контроль безпеки і конфіденційності для федеральних інформаційних систем і організацій https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
23. NIST 800-53 - Рекомендації по цифровій ідентифікації https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

15. Інформаційні ресурси

1. Цифровий інституціональний репозитарій Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут» [Ел. ресурс]. URL: https://dspace.library.khai.edu
2. Офіційний портал Верховної Ради України [Электрон. ресурс]. – Режим доступа: http://www.rada.gov.ua
3. Національна бібліотека України імені В. І. Вернадського [Ел. ресурс]. URL: http://www.nbuv.gov.ua
4. Національна бібліотека України імені Ярослава Мудрого [Ел. ресурс]. URL: https://nlu.org.ua/
5. Державна науково-технічна бібліотека [Ел. ресурс]. URL: http://www.gntb.gov.ua

6. Законодавство України [Электрон. ресурс]. – Режим доступа: http://zakon3.rada.gov.ua/laws
7. Державна служба спеціального зв’язку та захисту інформації України [Электрон. ресурс]. – Режим доступа: http://dstszi.kmu.gov.ua/dstszi/control/uk/index
8. Діяльність Адміністрації Держспецзв'язку у сфері кіберзахисту https://cip.gov.ua/ua/statics/cyber-protection
9. Перелік документів міжнародних організацій та країн-партнерів у сфері кіберзахисту https://cip.gov.ua/ua/news/perelik-dokumentiv-mizhnarodnikh-organizacii-ta-krayin-partneriv-usferi-kiberzakhistu
10. Нормативні документи системи ТЗІ https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi