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

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

**ЗАТВЕРДЖУЮ**

Гарант освітньої програми

__ _____ Дмитро Узун
(підпис) (ім'я та ПРІЗВИЩЕ)

«_31_» ____серпня____2025 р.

# СИЛАБУС ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Кваліфікаційна робота
(назва навчальної дисципліни)

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

**Спеціальність:** F5 Кібербезпека та захист інформації
(код і найменування спеціальності)

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

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

**Силабус введено в дію з 01.09.2025**

**Харків – 2025 р.**

Розробник (и): Узун Д.Д., професор, 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:


Іван ОЛЕФІРЕНКО
(підпис) (ім'я та ПРІЗВ

## 1. Загальна інформація про викладача

**ПІБ:** Узун Дмитро Дмитрович

**Посада:** професор

**Науковий ступінь:** кандидат технічних наук

**Вчене звання:** доцент

**Перелік дисциплін, які викладає:**

Домени кібербезпеки
Технології ДевСекОпс
Технології ДевОпс
Операційні системи
Безпека хмарних технологій
ДевОпс та хмарні технології

**Напрями наукових досліджень:**

Впровадження сучасних технологій автоматизації циклу розробки та забезпечення стану безпеки IT-проектів

**Контактна інформація:**

d.uzun@khai.edu

## 2. Опис навчальної дисципліни

| | |
|---|---|
| Форма здобуття освіти | Денна |
| Семестр | 3 |
| Мова викладання | Українська, англійська |
| Тип дисципліни | Обов'язкова (ОК11) |
| Обсяг дисципліни: кредити ЄКТС / кількість годин | 15 кредитів ЄКТС / 450 годин (0 аудиторних, з яких: СРЗ – 450) |
| 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 фахової підготовки, передбачених навчальним планом спеціальності. Є логічним продовженням дисципліни переддипломна практика (ОК10). |

## 3. Мета та завдання навчальної дисципліни

**Мета навчання:** визначення рівня підготовленості здобувача другого (магістерського) рівня вищої освіти до самостійного розв'язання складних задач дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки, на основі застосування системи теоретичних знань і практичних навичок, отриманих у процесі всього періоду навчання відповідно до вимог Стандарту вищої освіти за спеціальністю 125 «Кібербезпека» (наказ МОН № 332 від 18.03.2021 р.).

**Завдання:** систематизація, поглиблення та розширення теоретичних знань і практичних умінь, отриманих у процесі навчання за ОПП «Безпека інформаційних і комунікаційних систем»; проведення самостійного дослідження та/або інноваційної розробки з актуальної тематики кібербезпеки; застосування сучасних методів аналізу, моделювання, проектування та оцінювання систем захисту інформації; оформлення результатів дослідження відповідно до вимог академічної доброчесності та стандартів наукового письма; публічний захист отриманих результатів перед екзаменаційною комісією.

**Компетентності, які набуваються:**

***Інтегральна компетентність:*** Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

**Загальні компетентності (ЗК):**

- ЗК1. Здатність застосовувати знання у практичних ситуаціях.
- ЗК2. Здатність проводити дослідження на відповідному рівні.
- ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.
- ЗК4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
- ЗК5. Здатність спілкуватися з представниками інших професійних груп різного рівня.

**Спеціальні (фахові) компетентності (СК):**

- СК1 (КФ1). 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 (КФ2). 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 (КФ3). Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
- СК4 (КФ4). 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 (КФ5). 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.

- СК6 (КФ6). Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
- СК7 (КФ7). Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування кіберінцидентів.
- СК8 (КФ8). Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації, оцінювати ефективність їх використання.
- СК9 (КФ9). Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій в галузі інформаційної безпеки та/або кібербезпеки.
- СК10 (КФ10). Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
- 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.

**4. Програмні результати навчання**

В результаті виконання кваліфікаційної роботи магістра здобувачі мають досягти такі програмні результати навчання:

- 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.
- ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології 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 кіберінцидентів 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.
- ПРН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів у сфері інформаційної та/або кібербезпеки в цілому.
- 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.
- 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.
- ПРН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі.
- 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 в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях.
- 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 ІТ-інфраструктур.

**5. Зміст навчальної дисципліни**

**Модуль 1.**

**Змістовний модуль 1. Підготовка кваліфікаційної роботи магістра та її захист**

**Тема 1. Видача завдання та визначення теми дослідження.**

Обґрунтування актуальності та наукової/практичної значимості теми кваліфікаційної роботи. Визначення об'єкта, предмета, мети та завдань дослідження. Узгодження індивідуального завдання з науковим керівником. Планування виконання кваліфікаційної роботи.

**Тема 2. Аналіз предметної області та огляд літератури.**

Систематизація та критичний аналіз літературних джерел з питань, що вивчаються, включаючи вітчизняні та зарубіжні наукові публікації, стандарти та нормативно-правові документи у сфері кібербезпеки та захисту інформації. Ґрунтовне викладення сучасного стану проблеми. Робота з англомовними джерелами та міжнародними стандартами.

**Тема 3. Аналіз існуючих методів та рішень.**

Систематизація та порівняльний аналіз існуючих методологічних, технологічних, програмних, програмно-апаратних рішень з питань захисту інформаційних систем та/або кібербезпеки. Обґрунтування вибору підходу/рішення, що пропонується в кваліфікаційній роботі.

**Тема 4. Розроблення та/або дослідження запропонованого рішення.**

Опис та обґрунтування запропонованого методологічного, технологічного, програмного або програмно-апаратного рішення у сфері інформаційної та/або кібербезпеки. Проведення теоретичних та/або експериментальних досліджень, моделювання, розроблення прототипу або системи захисту. Оцінка точності та вірогідності отриманих результатів.

**Тема 5. Нормативно-правове та стандартизаційне забезпечення.**

Аналіз вимог національних та міжнародних нормативно-правових документів і стандартів (ДСТУ, ISO/IEC, NIST тощо) щодо запропонованого в кваліфікаційній роботі рішення. Забезпечення відповідності отриманих результатів вимогам чинного законодавства у сфері кібербезпеки та захисту інформації.

**Тема 6. Оформлення кваліфікаційної роботи.**

Оформлення пояснювальної записки відповідно до вимог ДСТУ 3008:2015 та правил оформлення навчальних і науково-дослідних документів. Проходження нормоконтролю. Перевірка кваліфікаційної роботи на предмет порушення академічної доброчесності (система виявлення плагіату). Розміщення кваліфікаційної роботи в репозитарії університету.

**Тема 7. Підготовка до захисту та публічний захист.**

Розроблення презентаційних матеріалів. Підготовка доповіді та відповідей на можливі запитання. Публічний захист кваліфікаційної роботи магістра перед екзаменаційною комісією.

## 6. Індивідуальні завдання

Тема кваліфікаційної роботи магістра має відповідати предметній області ОПП «Безпека інформаційних і комунікаційних систем» зі спеціальності 125 «Кібербезпека та захист інформації» та корелювати з тематикою переддипломної практики (ОК10). Теми кваліфікаційних робіт можуть бути запропоновані науковим керівником, стейкхолдерами (підприємствами-партнерами) або сформульовані самими здобувачами вищої освіти. Індивідуальне завдання на кваліфікаційну роботу погоджується з науковим керівником. Теми закріплюються за здобувачами, розглядаються та затверджуються на засіданні кафедри на початку третього семестру навчання.

Тематика кваліфікаційних робіт магістра охоплює, але не обмежується, такими напрямами:

- методи та засоби кіберзахисту інформаційно-комунікаційних систем і критичної інфраструктури;
- розробка та аналіз систем управління інформаційною безпекою (СУІБ);
- методи виявлення, аналізу та реагування на кіберінциденти;
- криптографічний та технічний захист інформації;
- безпека хмарних, розподілених та вбудованих систем;
- DevSecOps та безпечна розробка програмного забезпечення;
- аудит та моніторинг безпеки інформаційних систем;
- функційна безпечність інформаційно-керуючих систем.

## 7. Методи навчання

Виконання кваліфікаційної роботи здійснюється у формі самостійної науково-дослідної та/або інноваційно-проектної діяльності здобувача під керівництвом наукового керівника. Основні методи: проведення індивідуальних консультацій з науковим керівником; самостійна робота здобувача з науковою, методичною та нормативно-правовою літературою; застосування методів системного аналізу, математичного та комп'ютерного моделювання; виконання практичних досліджень та/або розробок; оформлення пояснювальної записки та ілюстративних матеріалів.

## 8. Методи контролю

Семестровий контроль проводиться у формі нормоконтролю, перевірки на наявність плагіату та публічного захисту кваліфікаційної роботи магістра перед екзаменаційною комісією. Поточний контроль виконання роботи здійснюється науковим керівником на систематичних консультаціях відповідно до індивідуального графіку виконання роботи.

## 9. Критерії оцінювання та розподіл балів, які отримують здобувачі освіти

**Таблиця 9.1 – Розподіл балів, які отримують здобувачі освіти**

| **Складові навчальної роботи** | **Сумарна кількість балів** |
|---|---|
| Тема 1. Видача завдання та визначення теми дослідження | 0…5 |
| Тема 2. Аналіз предметної області та огляд літератури | 0…10 |
| Тема 3. Аналіз існуючих методів та рішень | 0…10 |
| Тема 4. Розроблення та/або дослідження запропонованого рішення | 0…35 |
| Тема 5. Нормативно-правове та стандартизаційне забезпечення | 0…10 |
| Тема 7. Розроблення презентаційних матеріалів | 0…10 |
| Нормоконтроль | 0…5 |
| Перевірка на плагіат | 0…5 |
| Публічний захист | 0…10 |
| **Усього** | **0…100** |

**Таблиця 9.2 – Шкали оцінювання: бальна і традиційна**

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

### 9.1. Якісні критерії оцінювання

Кваліфікаційна робота магістра має відповідати вимогам дослідницького та/або інноваційного характеру, бути виконана відповідно до закріпленої теми, оформлена згідно затверджених вимог та своєчасно представлена до захисту. Автор кваліфікаційної роботи повинен продемонструвати: здатність самостійно ставити і вирішувати складні наукові та інженерні задачі у сфері кібербезпеки; вміння логічно та аргументовано викладати матеріал; коректне використання наукових методів і математичного апарату; проведення власних досліджень на відповідному рівні; навички узагальнення результатів та формулювання висновків; вміння ініціювати та обґрунтовувати інноваційні підходи до вирішення проблеми.

### 9.2. Критерії оцінювання роботи здобувача

Критеріями оцінювання кваліфікаційної роботи є:

- чіткість, повнота та наукова обґрунтованість постановки задачі дослідження;
- глибина та системність аналізу предметної області та існуючих рішень;
- оригінальність та новизна запропонованого рішення або отриманих результатів;
- коректність застосованих методів дослідження та обробки результатів;
- відповідність отриманих результатів вимогам стандартів і нормативних документів;
- правильне оформлення роботи відповідно до затверджених стандартів;
- відсутність ознак академічної недоброчесності (плагіату, фабрикації, фальсифікації);
- якість презентації та аргументованість відповідей на запитання комісії.

Оцінка «Задовільно» (60–74). Здобувач демонструє базовий рівень розуміння предметної області, виконав постановку задачі та провів огляд існуючих рішень; отримав певні результати дослідження під керівництвом наукового керівника; оформлення роботи загалом відповідає встановленим вимогам.

Оцінка «Добре» (75–89). Здобувач демонструє впевнене знання предметної області, самостійно виконав аналіз та порівняння існуючих рішень, отримав обґрунтовані результати дослідження; якісно оформлена робота, логічна і послідовна доповідь.

Оцінка «Відмінно» (90–100). Здобувач демонструє глибоке знання предметної області та пов'язаних дисциплін, самостійно отримав оригінальні наукові або практично значимі результати, обґрунтував їх та сформулював напрями подальших досліджень; доповідь структурована, переконлива, вичерпні відповіді на всі запитання комісії.

**10. Політика навчального курсу**

**Дотримання вимог академічної доброчесності.** Під час виконання кваліфікаційної роботи 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). Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації та фальсифікації. Виявлення ознак академічної недоброчесності є підставою для недопущення роботи до захисту.

**Оприлюднення кваліфікаційної роботи.** Кваліфікаційна робота магістра має бути розміщена в інституційному репозитарії університету відповідно до вимог законодавства та внутрішніх нормативних документів ХАІ.

**Вирішення конфліктів.** Порядок і процедури врегулювання конфліктних ситуацій регламентуються Кодексом етичної поведінки в Національному аерокосмічному університеті «Харківський авіаційний інститут» (https://khai.edu/ua/university/normativna-baza/ustanovchi-dokumenti/kodeks-etichnoi-povedinki/).

## 11. Методичне забезпечення

Навчально-методичний комплекс дисципліни розміщений у системі управління курсами кафедри комп'ютерних систем, мереж та кібербезпеки.
Система управління курсами кафедри [Ел. ресурс]. URL: https://elearn.csn.khai.edu

## 12. Рекомендована література

### Базова


- 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.
- 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
- Морозова О.І. та ін. Методичні вказівки до виконання кваліфікаційної роботи магістра зі спеціальності 125 «Кібербезпека». – Харків: ХАІ, 2024.
- Stalling W. Cryptography and Network Security: Principles and Practice. 8th ed. Pearson, 2021.
- Kim D., Solomon M. Fundamentals of Information Systems Security. 3rd ed. Jones & Bartlett Learning, 2018.
- NIST Cybersecurity Framework v2.0. – National Institute of Standards and Technology, 2024. URL: https://www.nist.gov/cyberframework
- ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.


### Допоміжна


- Kharchenko V. та ін. Safety and Security of Cyber-Physical Systems. Springer, 2022.
- ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки.
- ДСТУ EN 61508-1:2019 Функційна безпечність електричних, електронних, програмованих електронних систем.
- NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

- NIST SP 800-37 Rev. 2. Risk Management Framework for Information Systems and Organizations. URL: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
- ДСТУ 3008:2015. Інформація та документація. Звіти у сфері науки і техніки: Структура і правила оформлювання. – К.: ДП «УкрНДНЦ», 2016.
- ДСТУ 8302:2015. Інформація та документація. Бібліографічне посилання: Загальні положення та правила складання.

**Закони України**

- Закон України «Про основні засади забезпечення кібербезпеки України», 2163-VIII, чинний. URL: https://zakon.rada.gov.ua/laws/main/2163-19
- Закон України «Про інформацію», 2657-XII, чинний. URL: https://zakon.rada.gov.ua/laws/main/2657-12
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», 80/94-ВР, чинний. URL: https://zakon.rada.gov.ua/laws/main/80/94-вр
- Закон України «Про національну безпеку України», 2469-VIII, чинний. URL: https://zakon.rada.gov.ua/laws/main/2469-19
- Закон України «Про державну таємницю», 3855-XII, чинний. URL: https://zakon.rada.gov.ua/laws/show/3855-12

**Стандарти та технічне регулювання**

- Нормативні документи системи ТЗІ. URL: https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi
- Міжнародні стандарти ISO. URL: https://www.iso.org/ru/home.html
- Стандарти ETSI у сфері безпеки. URL: https://www.etsi.org/standards#Security
- Національні нормативні документи. URL: https://cip.gov.ua/ua/docs

## 13. Інформаційні ресурси

- Цифровий інституціональний репозитарій ХАІ. URL: https://dspace.library.khai.edu
- Офіційний портал Верховної Ради України. URL: https://rada.gov.ua
- Національна бібліотека України імені В. І. Вернадського. URL: http://www.nbuv.gov.ua
- Державна науково-технічна бібліотека. URL: http://www.gntb.gov.ua

- Законодавство України. URL: http://zakon3.rada.gov.ua/laws
- Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язок). URL: https://cip.gov.ua
- Діяльність Адміністрації Держспецзв'язку у сфері кіберзахисту. URL: https://cip.gov.ua/ua/statics/cyber-protection
- Перелік документів міжнародних організацій та країн-партнерів у сфері кіберзахисту. URL: https://cip.gov.ua/ua/news/perelik-dokumentiv-mizhnarodnikh-organizacii-ta-krayin-partneriv-u-sferi-kiberzakhistu
- NIST Cybersecurity Resource Center. URL: https://csrc.nist.gov
- ENISA – European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu