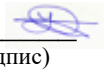
Міністерство освіти і науки України
Національний аерокосмічний університет
«Харківський авіаційний інститут»

**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

Стандартизація і сертифікація систем кібербезпеки
(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): 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:

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

## 1. Загальна інформація про викладача

**ПІБ:** Ілляшенко Олег Олександрович

**Посада:** доцент

**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 | 2 |
| Мова викладання | Українська, англійська |
| Тип дисципліни | Обов’язкова |
| Обсяг дисципліни: кредити ЄКТС/ кількість годин | 3 кредити ЄКТС / 90 годин (48 аудиторних, з яких: лекції – 32, практичні – 16; СРЗ – 42) |
| Види навчальної діяльності | Лекції, лабораторні заняття, самостійна робота |
| Види контролю | Семестровий контроль – іспит |
| Пререквізити | Дисципліна є обов’язковим компонентом освітньої програми і базується на знаннях, отриманих під час вивчення дисциплін у циклі загальної і професійної підготовки, передбачених навчальним планом спеціальності |

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

**Мета вивчення:** надання студентам необхідних знань і навичок щодо процесів стандартизації та сертифікації комп'ютерних систем інформаційної безпеки та/або кібербезпеки.

**Завдання:** формування у студентів фахових знань щодо існуючих національних та міжнародних стандартів з технічного регулювання кібербезпеки, процедур, методів та засобів підтримки стандартизації та сертифікації систем кібербезпеки.

**Компетентності, які набуваються.**

**Інтегральна компетентність:**

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

**Загальні компетенції:**

– ЗК1. Здатність до адаптації та дій в новій ситуації.
– 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 обгрунтовані рішення.

**Спеціальні компетенції:**

– 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 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 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 та 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.

**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.

– 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.

– ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

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

– 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.

– 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.

– 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.

– ПРН24. Аналізувати та оцінювати показники функційної безпечності інформаційнокеруючих систем та обґрунтовувати рекомендації щодо її забезпечення відповідно вимогам нормативних документів.

## 4. Зміст навчальної дисципліни

**Модуль 1. Стандартизація та сертифікація та методів та засобів захисту інформації.**

**Змістовний модуль 1. Науково-методичні основи стандартизації.**

**Тема 1.** Суть стандартизації та організація стандартизації в Україні і світі.

**Анотація:** Головні принципи стандартизації. Етапи стандартизації. Форми стандартизації та подання стандартів. Порядок розробки стандартів. Організаційна система стандартизації. Особливості стандартизації засобів захисту інформації. Суть стандартизації та організація стандартизації в галузі захисту інформації в Україні та світі. Міжнародні та національні організації зі стандартизації у сфері захисту інформації. Положення про кібербезпеку Європейського Союзу. Регулювання питань кібербезпеки в США. Нормативно-правова база державної експертизи у сфері ТЗІ. Кібербезпека в сфері захисту критичної інфраструктури.

**Тема лекції 1:** Стандартизація: форми, роль.

**Тема лекції 2:** Порядок розроблення національних та міжнародних стандартів в галузі захисту інформації.

**Самостійна робота здобувача:** Опрацювання лекційного матеріалу, підготовка короткого огляду основних стандартів кібербезпеки.

**Змістовний модуль 2. Методологічні основи забезпечення інформаційної безпеки**.

**Тема 2.** Міжнародні стандарти з основ забезпечення безпеки інформації та кібербезпеки.

**Анотація:** нормативні документі із методологічних основ забезпечення інформаційної безпеки. Базова технічна модель безпеки ІТ-систем. Поняття інформаційно-керуючих систем. Життєвий цикл, верифікація, сертифікація та ліцензування систем критичного застосування та систем, важливих для безпеки. Процедури сертифікації та ліцензування. Основи сертифікації та ліцензування діяльності в галузі захисту інформації. Показники оцінювання запевнення кібербезпеки за національними стандартами. Процедура сертифікації за національними стандартами. Вимоги національних стандартів НД ТЗІ 2.5-004-1999, НД ТЗІ 2.6-001-2011, НД ТЗІ 2.7-010-2009.

**Тема лекції 3:** Поняття інформаційно-керуючих систем.

**Тема лекції 4:** Процедури сертифікації та ліцензування інформаційно-керуючих систем, важливих для безпеки.

**Самостійна робота здобувача:** Аналіз вимог національних стандартів НД ТЗІ.

**Тема 3.** Стандартизація кібербезпеки та функційної безпечності в системах промислової автоматизації.

**Анотація:** поняття функційної безпечності. Різновиди безпеки та взаємозв’язок між ними. Функційна безпечність, інформаційна безпека,

кібербезпека. Основні міжнародні стандарти механізмів безпеки. Основні стандарти та керівні принципи з оцінювання функційної безпечності. Основні стандарти та керівні принципи з оцінювання інформаційної безпеки та кібербезпеки. Класифікація нормативних документів. Призначення стандартів. Основні визначення. Фреймворк для сумісного розроблення захищенного продукту з урахуванням функціональної та інформаційної безпеки систем. Кібербезпека індустріальних систем. Велика безпека.

**Тема лекції 5:** Поняття безпеки. Різновиди безпеки та взаємозв'язок між ними. Функційна безпечність, інформаційна безпека, кібербезпека.

**Тема лекції 6:** Основні стандарти та керівні принципи з оцінювання функційної безпечності. Класифікація нормативних документів.

**Тема лекції 7:** Основні стандарти та керівні принципи з оцінювання інформаційної безпеки та кібербезпеки. Класифікація нормативних документів

**Самостійна робота здобувача:** Аналітичне дослідження понять функційної безпечності, інформаційної безпеки та кібербезпеки, визначивши їх відмінності та взаємозв'язок на основі міжнародних стандартів. Ааліз ключових стандартів з оцінювання функційної безпечності та кібербезпеки, класифікація нормативних документів та визначення їх призначення. Здійснення порівняльного аналізу safety- та security-підходів і демонстрація їх застосування на прикладі промислової системи. Результат роботи представляється у вигляді структурованої аналітичної записки з таблицями, схемами та обґрунтованими висновками.

**Тема 4.** Класифікація підходів для обґрунтування безпеки.

**Анотація:** Організація процесу розроблення обґрунтувань безпеки. Основні нотації, що застосовуються при обґрунтуванні безпеки за допомогою кейсів: модель аргументації Тулміна, нотація ASCAD, нотація GSN, модель аргументації Trust-IT.

**Тема лекції 8:** Поняття assurance та confidence. Вибір підходу для запевнення безпеки. Коректність та ефективність

**Тема лекції 9:** Модель аргументації Тулміна.

**Тема лекції 10:** Нотація ASCAD.

**Тема лекції 11:** Нотація GSN.

**Тема лекції 12:** Модель аргументації Trust-IT.

**Самостійна робота здобувача:** Аналіз поняття assurance та confidence, обґрунтування вибору підходу до запевнення безпеки та оцінка його коректносі і ефективності для заданої системи. Порівняння моделі аргументації Тулміна, нотації ASCAD і GSN, Trust-IT, визначивши їх структуру, переваги та обмеження. Результатом роботи представляється у вигляді побудованого фрагмену обґрунтування безпеки (Assurance Case) для прикладної системи з використанням однієї з розглянутих нотацій та коротким аналітичним поясненням вибору.

**Тема 5.** Функціональний підхід до оцінювання кібербезпеки. Підтримка сертифікації систем кібербезпеки за допомогою кейсів.

**Анотація:** аналіз міжнародного стандарту ISO/IEC 15408. Побудова профілю захисту. Формування вимог до результату оцінювання запевнення безпеки. Формування вимог до кейсу безпеки. Поняття гарантій та запевнення безпеки. Критерії оцінки безпеки інформаційних технологій. Міжнародні стандарти з запевнення ІТ безпеки. Використання покращеного кейсу запевнення безпеки Advanced Security Assurance Case (ASAC) для оцінювання кібербезпеки. Онтологічна моделі опису взаємозв'язку між поняттями запевнення, оцінювання та забезпечення вимог до кібербезпеки. Класифікація вимог до кібербезпеки. Вимоги до побудови покращеного кейсу запевнення ASAC. Інформаційні засоби підтримки процесу кейс-оцінювання.

**Тема лекції 13:** Обгрунтування безпеки. Оцінювання запевнення безпеки. Кейс запевнення безпеки Assurance Case.

**Тема лекції 14:** Формування вимог до представлення результатів оцінювання кібербезпеки у вигляді кейсу.

**Тема лекції 15:** Інформаційні засоби підтримки процесу кейс-оцінювання.

**Самостійна робота здобувача:** Аналіз вимог національних стандартів НД ТЗІ щодо оцінювання та запевнення кібербезпеки, визначити їх відповідність підходам ISO/IEC 15408 та принципам формування профілю захисту і кейсу запевнення безпеки (Assurance Case / ASAC). Результатом роботи має бути структурований аналіз із класифікацією вимог, визначенням рівнів гарантій та побудовою узагальненої моделі представлення результатів оцінювання у вигляді кейсу запевнення безпеки.

**Тема 6.** Методи оцінювання кібербезпеки, що використовуються при сертифікації систем, важливих для безпеки.

**Анотація:** використання різноманітних методів при стандартизації та сертифікації систем критичного застосування, важливих для безпеки: FMEA/FMECA/FMEDA/IMECA (родина аналізу видів та наслідків відмов/критичності відмов/діагностовності відмов/вторгнень), HAZOP (дослідження небезпек та працездатності), RBD (структурна схема надійності). Структура та особливості застосування. Приклади застосування.

**Тема лекції 16:** Методи оцінювання безпеки, що використовуються при сертифікації систем, важливих для безпеки

**Самостійна робота здобувача:** Аналітичний огляд методів FMEA/FMECA/FMEDA, HAZOP та RBD, визначення можливості і доцільності їх застосування для оцінювання кібербезпеки систем, важливих для безпеки, а також обґрунтувати обмеження їх використання у межах чинної нормативної бази України.

## 5. Індивідуальні завдання

Не передбачено.

## 6. Методи навчання

Проведення аудиторних лекцій, лабораторних робіт, консультацій, а також самостійна робота здобувачів з використанням відповідних матеріалів (п.11, 12).

## 7. Методи контролю

Проведення поточного контролю, підсумковий контроль у вигляді іспиту.

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

Таблиця 8.1 – Розподіл балів, які отримують здобувачі освіти

| Складові навчальної роботи | Бали за одне заняття (завдання) | Кількість занять (завдань) | Сумарна кількість балів |
|---|---|---|---|
| **Змістовний модуль 1** | | | |
| Виконання і захист лабораторних робіт | 0…1 | 2 | 0…40 |
| **Змістовний модуль 2** | | | |
| Виконання і захист лабораторних робіт | 0…20 | 2 | 0…40 |
| Підсумковий контроль | 0…20 | 1 | 0…20 |
| **Усього за семестр** | | | **0…100** |

Таблиця 8.2 – Шкали оцінювання: бальна і традиційна

| Сума балів | Оцінка за традиційною шкалою | |
|---|---|---|
| | Іспит, диференційний залік | Залік |
| 90 – 100 | Відмінно | Зараховано |
| 75 – 89 | Добре | |
| 60 – 74 | Задовільно | |
| 0 – 59 | Незадовільно | Не зараховано |

### Критерії оцінювання роботи здобувача протягом семестру

1. **Задовільно (60-74).** Показати мінімум знань та умінь. Захистити не менше 80% від усіх завдань практичних занять. Знати основні міжнародні та національні нормативні документи зі стандартизації та сертифікації інформаційних систем.
2. **Добре (75-89).** Твердо знати необхідний обсяг знань для одержання позитивної оцінки, захистити не менше 90% завдань практичних занять. Уміти використовувати практичні навички з використання міжнародних та національних нормативних документів зі стандартизації та сертифікації інформаційних систем для розроблення елементів профілю захисту у

відповідності до вимог міжнародного стандарту ISO/IEC 15408. Знати основні етапи побудови ASAC.

3. **Відмінно (90-100).** Повно знати основний та додатковий матеріал. Уміти застосовувати навички для розроблення елементів профілю захисту у відповідності до вимог міжнародного стандарту ISO/IEC 15408. Вміти побудовувати та застосовувати ASAC для підтримки процесу сертифікації кібербезпеки IT-продуктів.

## 9. Політика навчального курсу

**Відвідування занять.** Інтерактивний характер курсу передбачає обов'язкове відвідування лабораторних занять. Здобувачі освіти, які за певних обставин не можуть відвідувати лабораторні 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 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. 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.

**Вирішення конфліктів.** Порядок і процедури врегулювання конфліктів 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=2132

## 11. Рекомендована література

1) **Базова**


1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. Харків. Форт. 2013р. , 878с.
2. За редакцією Горбенко І.Д., Горбенко Ю.І. «Побудування та аналіз систем, протоколів та засобів криптографічного захисту інформації». . Монографія. Харків. Форт. 2015 , 902с.
3. За редакцією Горбенко І.Д., Горбенко Ю.І. «Побудування та аналіз систем, протоколів та засобів криптографічного захисту інформації». Електронна версія. Монографія. Харків. Форт. 2015, 902 с.
4. Методи і засоби забезпечення виконання вимог до кібербезпеки систем на програмовній логіці. Methods and Means of the Cybersecurity Requirements Compliance Ensuring for Programmable Logic Systems : монографія / О. О. Ілляшенко; М-во освіти і науки України, Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т" ; за ред. В. С. Харченка. - Харків. - Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т", 2019.
5. Ілляшенко О., Бабешко Є., Харченко В. Кібербезпека індустріальних систем. [Ел. ресурс]. URL: https://tk185.appau.org.ua/whitepapers/aCampus-whitepaper-cybersecurity+++.pdf
6. Бабешко Є., Ілляшенко О., Харченко В. Функційна безпека індустріальних систем. [Ел. ресурс]. URL: https://tk185.appau.org.ua/whitepapers/aCampus-whitepaper-IEC-61508+++.pdf
7. Інтернет речей для індустріальних і гуманітарних застосунків. У трьох томах. Том 1. Основи і технології / За ред. В. С. Харченка. – Міністерство освіти і науки України, Національний аерокосмічний університет ХАІ, 2019. – 605 с https://aliot.eu.org/wp-content/uploads/2020/07/ALIOT_Multi-Book_Volume1_web.pdf
8. А.В. Лєншин, О. О. Ілляшенко, О.В. Потій, Методи та засоби оцінювання гарантій ІТ безпеки. Тренінг / під ред. В.С. Харченко – Міністерство освіти та науки України, Національний аерокосмічний університет ім. Н.Е. Жуковського «ХАІ». 2017. – 100 с. https://serein.eu.org/wp-content/uploads/2017/10/CT3-Techniques-and-tools-for-evaluation-of-IT-security-assurance.pdf
9. V. Sklyar, O. Illiashenko, V. Kharchenko, N. Zagorodna, R. Kozak, O. Vambol, S. Lysenko, D. Medzatyi, O. Pomorova. Secure and resilient computing for industry and human domains. Volume 1. Fundamentals of security and resilient computing / Edited by Kharchenko V. S. – Department of Education and Science of Ukraine, National Aerospace University named after N. E. Zhukovsky “KhAI”, 2017. https://serein.eu.org/wp-content/uploads/2017/10/Volume-1.-Fundamentals-of-secure-and-resilient-computing.pdf
10. D2.9 ECHO CYBERSECURITY CERTIFICATION SCHEME https://echonetwork.eu/wp-content/uploads/2021/03/D2.9-ECHO-Cybersecurity-Certification-Scheme.pdf

11. Colabuono, C. et al. (2022). Approach to Sector-Specific Cybersecurity Schemes: Key Elements and Security Problem Definition. In: Dziech, A., Mees, W., Niemiec, M. (eds) Multimedia Communications, Services and Security. MCSS 2022. Communications in Computer and Information Science, vol 1689. Springer, Cham. https://doi.org/10.1007/978-3-031-20215-5_9

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

## 12. Інформаційні ресурси

1. Національна бібліотека України імені В. І. Вернадського [Ел. ресурс]. URL: http://www.nbuv.gov.ua
2. Національна бібліотека України імені Ярослава Мудрого [Ел. ресурс]. URL: https://nlu.org.ua/
3. Державна науково-технічна бібліотека [Ел. ресурс]. URL: http://www.gntb.gov.ua
4. Законодавство України [Ел. ресурс]. URL: http://zakon3.rada.gov.ua/laws
5. Державна служба спеціального зв'язку та захисту інформації України ДСТЗІ. Національні нормативні документи [Ел. ресурс]. URL: https://cip.gov.ua/ua/docs
6. Державна служба спеціального зв'язку та захисту інформації України ДСТЗІ. Захист інформації [Ел. ресурс]. URL: https://cip.gov.ua/ua/statics/zakhist-informaciyi
7. Державна служба спеціального зв'язку та захисту інформації

України ДСТЗІ. Діяльність Адміністрації Держспецзв'язку у сфері кіберзахисту [Ел. ресурс]. URL: https://cip.gov.ua/ua/statics/cyber-protection
8. 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
9. Нормативні документи системи ТЗІ https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi
10. CERT-UA. Загальні правила обміну інформацією про кіберінциденти: [Ел. ресурс]. URL: https://cert.gov.ua/recommendation/4256181
11. CERT-UA. Перелік категорій кіберінцидентів. [Ел. ресурс]. URL: https://cert.gov.ua/recommendation/16904
12. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Харків : Видавництво. ХНЕУ, 2013. – 476 с. http://kist.ntu.edu.ua/textPhD/tzi.pdf
13. IEEE Xplore Institute of Electrical and Electronics Engineers [Ел. ресурс]. URL: https://ieeexplore.ieee.org/Xplore/home.jsp

**1) 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

**2) 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".

**3) 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".

**4) Нормативні документи**

1. НД ТЗІ 2.7-008-08 "Вимоги та рекомендації із забезпечення захисту мовної інформації від витоку акустичним та вібро-акустичним каналами. Методичні вказівки."

2. НД ТЗІ 2.3-017-08 "Методика контролю захищеності мовної інформації від витоку акустичним та вібро-акустичним каналами"

3. НД ТЗІ 2.2-006-08 "Захист інформації на об'єкті інформаційної діяльності. Норми протидії технічній розвідці в акустичному і вібро-акустичному каналах витоку мовної інформації".

4. НД ТЗІ 2.2-003-06 "Протидія технічним розвідкам. Норми з протидії засобам радіолокаційної розвідки"

5. НД ТЗІ 2.3-010-06 "Протидія технічним розвідкам. Методика контролю ефективності протидії засобам радіолокаційної розвідки"

6. НД ТЗІ 2.4-003-06 "Протидія технічним розвідкам. Рекомендації щодо протидії засобам радіолокаційної розвідки"

7. НД ТЗІ 2.3-011-06 "Протидія технічним розвідкам. Методики контролю виконання норм з протидії засобам фотографічної та оптико-електронної розвідок".

8. НД ТЗІ 2.4-004-06 "Протидія технічним розвідкам. Рекомендації з протидії засобам фотографічної та оптико-електронної розвідок".

9. НД ТЗІ 1.6-002-03 "Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації"

10. НД ТЗІ 2.5-010-03 "Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу"

11. 11. НД ТЗІ 2.5-008-2002 "Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2"

12. НД ТЗІ 4.7-002-01 "Визначення захищеності мовної інформації від витоку акустичним і вібро-акустичним каналами. Методичні вказівки"

13. НД ТЗІ 3.6-001-2000 "Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів тех.-нічного захисту інформації від несанкціонованого доступу"

14. НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі"

15. НД ТЗІ Р-001-2000 "Засоби активного захисту мовної інформації з акустичними та вібро-акустичними джерелами випромінювання. Класифікація та загальні технічні вимоги. Рекомендації"

16. НД ТЗІ 1.5-001-2000 "Радіовиявлювачі. Класифікація. Загальні технічні вимоги"

17. НД ТЗІ 2.5-006-99 "Класифікатор засобів копіювально-розмножувальної техніки"

18. НД ТЗІ 2.7-002-99 "Методичні вказівки з використання засобів копіювально-розмножувальної техніки"

19. НД ТЗІ 1.1-001–99 "Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення".

20. НД ТЗІ 2.5-001–99 "Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту"

21. НД ТЗІ 2.5-002-99 "Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту"

22. НД ТЗІ 2.5-003-99 "Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту"

23. НД ТЗІ 2.7-001-99 "Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт"

24. НД ТЗІ 3.7-002-99 "Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова)"

25. НД ТЗІ 1.1-002-99 "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу"

26. НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу"

27. НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу"

28. НД ТЗІ 3.7-001-99 "Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі"

**5) Стандарти**

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