Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
"Харківський авіаційний інститут"

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
_____ В. В. Павліков
(підпис) (ініціали та прізвище)
«__» _____ 2020 р.
Відділ аспірантури і докторантури

РОБОЧА ПРОГРАМА ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Формальні методи аналізу безпеки
(назва навчальної дисципліни)

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

Спеціальність: 125 «Кібербезпека»
(код та найменування спеціальності)

Освітньо-наукова програма: «Кібербезпека»
(назва освітньої програми)

Рівень вищої освіти: третій (освітньо-науковий)

Форма навчання: денна

Харків 2020 рік

РОБОЧА ПРОГРАМА
ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Формальні методи аналізу безпеки
(назва дисципліни)

для здобувачів за спеціальністю 125 "Кібербезпека"

освітньо-наукової програми "Кібербезпека"

«26» 08 2020 р., – 14 с.

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

Гарант ОНП доцент, к.т.н. _____ Колісник М.О.
(посада, науковий ступінь та вчене звання) (підпис) (прізвище та ініціали)

Протокол №1 від «27» серпня 2020 р. засідання кафедри № 503

Завідувач кафедри д.т.н., професор _____ Харченко В. С.
(науковий ступінь та вчене звання) (підпис) (прізвище та ініціали)

ПОГОДЖЕНО:

Завідувач відділу
аспірантури і докторантури _____ В. Б. Селевко

Голова наукового товариства
студентів, аспірантів,
докторантів і молодих вчених _____ Т. П. Старовойт

1. Опис навчальної дисципліни

<table>
<tr><td>Найменування показників</td><td>Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td>Характеристика навчальної дисципліни (денна форма навчання)</td></tr>
<tr><td>Кількість кредитів – 5</td><td rowspan="8">Галузь знань
12 «Інформаційні технології»
(шифр та найменування)

Спеціальність
125 «Кібербезпека»
(код та найменування)

Освітньо-наукова програма
«Кібербезпека»
(найменування)

Рівень вищої освіти:
третій (освітньо-науковий)</td><td>Вибіркова</td></tr>
<tr><td>Кількість модулів – 1</td><td rowspan="2">Навчальний рік
2020/2021</td></tr>
<tr><td>Кількість змістовних модулів – 2</td></tr>
<tr><td>Індивідуальне завдання: немає</td><td rowspan="2">Семестр: 4-й</td></tr>
<tr><td>Загальна кількість годин – 68/150</td></tr>
<tr><td rowspan="5">Кількість тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи студента – 4,8</td><td>Лекції
34 год.</td></tr>
<tr><td>Практичні, семінарські
0 год.</td></tr>
<tr><td>Лабораторні
34 год.</td></tr>
<tr><td>Самостійна робота
82 год.</td></tr>
<tr><td>Індивідуальні завдання: 0 год.</td></tr>
<tr><td colspan="2">Вид контролю: іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить – 68/82

2. Мета та завдання навчальної дисципліни

1. Мета вивчення: надання аспірантам необхідних знань та навичок їх застосування для проведення аналізу безпеки інформаційних технологій та комп'ютеризованих систем з використанням формальних і напівформальних методів для проведення наукових досліджень.

2. Завдання: підготовка фахівців, здатних застосовувати і удосконалювати кейс-орієнтовані методи і засоби аналізу і оцінювання функціональної і кібербезпеки комп'ютеризованих систем з використанням формальних і напівформальних процедур.

3. Програмні компетентності. Дисципліна має допомогти сформувати у студентів такі компетентності:

- здатність до абстрактного мислення, аналізу та синтезу;
- здатність до пошуку, оброблення та аналізу інформації з різних джерел;
- здатність розробляти проекти та управляти ними;
- здатність застосовувати сучасні інформаційні технології, бази даних та інші електронні ресурси, спеціалізоване програмне забезпечення у науковій та навчальній діяльності;
- здатність виявляти, ставити та вирішувати проблеми дослідницького характеру в сфері кібербезпеки.

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

- формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень (опитувань, спостережень та інше) і математичного та/або комп'ютерного моделювання, наявні літературні дані;
- розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у кібербезпеці та дотичних міждисциплінарних напрямах;
- застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи;
- знати сучасні підходи та засоби моделювання досліджуваних об'єктів та процесів управління, в тому числі в аерокосмічній галузі, вміти створювати нові, вдосконалювати та розвивати методи математичного і комп'ютерного моделювання складних систем, оптимізації та прийняття рішень;
- знати, розуміти та вміти застосовувати методи та засоби створення інформаційних технологій та програмного забезпечення розподілених систем, Інтернету речей, хмарних обчислень, систем штучного інтелекту, віртуальної реальності у різних предметних областях, в тому числі в аерокосмічній галузі.

5. Міждисциплінарні зв'язки.

Матеріал дисципліни базується на знаннях, отриманих під час вивчення дисциплін із циклу обов'язкових компонент, а саме «ІТ в практиці наукових досліджень», «Наукові англомовні комунікації», «Теорія і технології критичного комп'ютингу», «Теорія і методи зеленої ІТ-інженерії».

Матеріал, засвоєний під час вивчення цієї дисципліни, є базою для підготовки дисертаційної роботи.

3. Програма навчальної дисципліни

МОДУЛЬ 1

Змістовний модуль 1. Поняття безпеки. Класифікація підходів для оцінювання та обґрунтування безпеки. Застосування стандартів для аналізу безпеки.

Тема 1. Поняття інформаційно-керуючих систем. Процедури сертифікації та ліцензування.

Визначаються основні поняття ІКС, стандартизації, життєвого циклу ІКС. V-модель життєвого циклу.

Тема 2. Поняття безпеки. Різновиди безпеки та взаємозв'язок між ними. Функціональна, інформаційна, кібербезпека.

Визначаються основні поняття безпеки (функціональна, інформаційна, кібербезпека) та взаємозв'язки між ними. Основні нормативні документи з регулювання функціональної, інформаційної та кібербезпеки по галузях.

Тема 3. Класифікація підходів для обґрунтування безпеки.

Визначаються три підходи для обґрунтування безпеки: підхід, заснований на застосуванні стандартів ціле-орієнтований підхід, та підхід, заснований на оцінці вразливостей.

Тема 4. Основні стандарти та керівні принципи з оцінювання функціональної безпеки. Класифікація нормативних документів.

Рівень цілісності функціональної безпеки (англ. Safety Integrity Level). Оцінювання функціональної безпеки за стандартом IEC 61508:2010.

Тема 5. Основні стандарти та керівні принципи з оцінювання інформаційної та кібербезпеки. Класифікація нормативних документів.

Рівень оцінювання запевнення інформаційної безпеки (англ. Evaluation Assurance Level). Загальні Критерії. Оцінювання інформаційної безпеки за стандартами ДСТУ ISO/IEC 15408-1:2017, ДСТУ ISO/IEC 15408-2:2017, ДСТУ ISO/IEC 15408-3:2017.

Змістовний модуль 2. Кейс-орієнтовне оцінювання безпеки як напрямок ціле-орієнтовного підходу до оцінювання безпеки. Методи та засоби аналізу вразливостей та загроз безпеки.

Тема 6. Модель аргументації Тулміна.

Основні поняття моделі аргументації Тулміна як базової моделі для проведення кейс-оцінювання. Система позначень. Структура типового аргументу.

Тема 7. Нотація ASCAD.

Поняття обґрунтування безпеки компанії Аделард (англ. Adelard safety case development, ASCAD). Структура аргументу, модель аргументації ASCAD.

Тема 8. Нотація GSN.

Поняття нотації структурування цілі (англ. goal structuring notation, GSN). Основні елементи, модель аргументації, ціле-орієнтована структура.

Тема 9. Модель аргументації Trust-IT.

Обґрунтування довіри (кейс довіри). Модель аргументу Trust-IT а її структурні елементи.

Тема 10. Кейс запевнення безпеки Assurance Case.

Еволюція поняття «запевнення» безпеки. Покращений кейс запевнення інформаційної безпеки (англ. advanced security assurance case, ASAC)

Тема 11. Формування вимог до представлення результатів оцінювання кібербезпеки у вигляді кейсу.

Аналіз вимог до структури кейсу та до результату оцінювання безпеки за допомогою кейсу.

Тема 12. Інформаційні засоби підтримки процесу кейс-оцінювання

Середовище розробки ASCE. Інструментальний засіб Emphasis. Інструментальні засоби Cobra і КОНДОР. Середовище моделювання Atego GSN Modeler.

Тема 13. Родина аналізу видів та наслідків відмов

Аналіз видів та наслідків відмов (англ. FMEA). Аналіз видів, наслідків та критичності відмов (англ. FMECA). Аналіз видів, наслідків та критичності програмних відмов (англ. SFMECA). Аналіз видів, наслідків та критичності процесних відмов (англ. PFMECA). Аналіз видів, наслідків та критичності проектних відмов (англ. DFMECA).Аналіз видів, наслідків та діагностування відмов (англ. FMECA). Аналіз видів, наслідків та критичності вразливостей (англ. FMVEA). Аналіз видів, наслідків та критичності втручань (англ. IMECA).

Тема 14.

Структура та особливості застосування аналізу HAZOP.

Тема 15.

Структура та особливості застосування аналізу RBD.

Модульний контроль.

4. Структура навчальної дисципліни

Назви змістовних модулів і тем	Кількість годин				
	Денна форма				
	Усього	У тому числі			
		л	п	лаб.	с.р.
1	2	3	4	5	6
Модуль 1					
Змістовний модуль 1. ***Поняття безпеки. Класифікація підходів для оцінювання та обґрунтування безпеки. Застосування стандартів для аналізу безпеки***					
Тема 1. Поняття інформаційно-керуючих систем. Поняття розробки та верифікації. Процедури сертифікації та ліцензування	12	2		2	8
Тема 2. Поняття безпеки. Різновиди безпеки та взаємозв'язок між ними. Функціональна, інформаційна, кібербезпека	15	4		3	8
Тема 3. Класифікація підходів для обґрунтування безпеки	15	4		3	8
Тема 4. Основні стандарти та керівні принципи з оцінювання функціональної безпеки. Класифікація нормативних документів	16	4		4	8
Тема 5. Основні стандарти та керівні принципи з оцінювання інформаційної та кібербезпеки. Класифікація нормативних документів. Модульний контроль	16	4		4	8
Разом за змістовним модулем 1	**74**	**18**		**16**	**40**
Змістовний модуль 2. ***Кейс-орієнтовне оцінювання безпеки як напрямок ціле-орієнтовного підходу до оцінювання безпеки. Методи та засоби аналізу вразливостей та загроз безпеки***					
Тема 6. Модель аргументації Тулміна	4	1		1	2
Тема 7. Нотація ASCAD	4	1		1	2
Тема 8. Нотація GSN	4	1		1	2
Тема 9. Модель аргументації Trust-IT	4	1		1	2
Тема 10. Кейс запевнення безпеки Assurance Case	11	2		2	7
Тема 11. Формування вимог до представлення результатів оцінювання кібербезпеки у вигляді кейсу	13	2		4	7
Тема 12. Інформаційні засоби підтримки процесу кейс-оцінювання	10	2		3	5

Тема 13. Родина аналізу видів та наслідків відмов	9	2		2	5
Тема 14. Структура та особливості застосування аналізу HAZOP	9	2		2	5
Тема 15. Структура та особливості застосування аналізу RBD Модульний контроль	9	2		2	5
Разом за змістовним модулем 2	**76**	**16**		**18**	**42**
Усього годин	**150**	**34**		**34**	**82**

5. Теми семінарських занять

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

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Огляд основних понять ІКС. Поняття розробки та верифікації	2
2	Різновиди безпеки та взаємозв'язок між ними	2
3	Класифікація підходів для обгрунтування безпеки	2
4	Основні стандарти та керівні принципи з оцінювання функціональної безпеки	2
5	Основні стандарти та керівні принципи з оцінювання інформаційної та кібербезпеки	2
6	Наукові дослідження за допомогою моделі аргументації Тулміна	2
7	Наукові дослідження за допомогою нотації ASCAD	2
8	Наукові дослідження за допомогою нотації GSN	2
9	Наукові дослідження за допомогою моделі аргументації Trust-IT	2
10	Наукові дослідження за допомогою кейсу запевнення безпеки Assurance Case	4
11	Формування вимог до представлення результатів оцінювання кібербезпеки у вигляді кейсу	3
12	Наукові дослідження за допомогою інформаційних засобів підтримки процесу кейс-оцінювання	2
13	Родина аналізу видів та наслідків відмов	3
14	Структура та особливості застосування аналізу HAZOP	2
15	Структура та особливості застосування аналізу RBD	2
	Разом	**34**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Ознайомитись з міжнародними стандартами в сфері функціональної, інформаційної та кібербезпеки	10
2	Опрацювати статтю, опубліковану в фаховому виданні України за темою дисертаційного дослідження і зробити рецензію на неї	15
3	Опрацювати три англомовних наукових статті з описом застосування методів та засобів аналізу функціональної безпеки та кібербезпеки для предметної галузі за темою дисертаційного наукового дослідження і зробити рецензію на них	20
4	Підготовити науково-дослідну статтю за результатами застосування методів аналізу безпеки для об'єкту дослідження у відповідності до теми дисертаційного дослідження	37
	Разом	**82**

9. Індивідуальні завдання

Не передбачено навчальним планом

10. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, консультацій, а також самостійна робота аспірантів за матеріалами, опублікованими кафедрою.

11. Методи контролю

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

12. Розподіл балів, які отримують аспіранти

12.1. Розподіл балів, які отримують аспіранти (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Робота на лекціях	0…1	9	0…9
Виконання лабораторних робіт	0…5	2	0...10
Модульний контроль	0…11	1	0…11
Змістовний модуль 2			
Робота на лекціях	0…1	8	0…8
Виконання лабораторних робіт	0…5	2	0…10
Написання і рецензування статей	0…20	2	0…40
Модульний контроль	0…10	1	0…12
Усього за семестр			**0…100**

Семестровий контроль (іспит) проводиться у разі відмови аспіранта від балів поточного тестування й за наявності допуску до іспиту. Під час складання семестрового іспиту аспірант має можливість отримати максимум 100 балів.

Білет для іспиту складається з двох теоретичних питання (0…30 балів за кожне питання) та одно практичне завдання (0…40 балів).

12.2. Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки.

Аспірант повинен знати:

- основні етапи розробки та верифікації інформаційно-керуючих систем;
- різновиди безпеки та взаємозв'язок між ними;
- основні міжнародними стандарти та керівні принципи в сфері функціональної, інформаційної та кібербезпеки;
- класифікацію підходів для аналізу та обгрунтування безпеки;
- знати принципи рецензування і написання наукових статей.

Необхідний обсяг вмінь для одержання позитивної оцінки.

Аспірант повинен вміти:

– вміти здійснювати рецензування статей і писати наукові статті, перевіряти їх на плагіат;

– вміти користуватись сучасними інформаційними технологіями для проведення наукових досліджень;

– використовувати сучасні методи та засоби формального аналізу безпеки інформаційно-керуючих систем.

12.3 Критерії оцінювання роботи аспіранта протягом семестру

Задовільно (60-74). Аспірант виявляє не достатньо глибоке знання програмного матеріалу, володіє основним понятійним апаратом, але допускає принципові помилки. Виконав рецензування двох статей: україномовної та англомовної. Знає базові поняття, що стосуються інформаційних технологій і вміє використовувати сучасні інформаційні технології.

Добре (75-89). Аспірант виявляє достатньо глибоке знання програмного матеріалу, володіє понятійним апаратом, вміє аргументувати свої відповіді, але у відповідях допускаються неточності, які впливають на чіткість. Виконав не менше 90% лабораторних робіт. Отримав з редакції наукового журналу, зазначеного у переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора технічних наук та доктора філософії підтвердження про прийняття до публікації наукової статті (у співавторстві) за тематикою дисертаційних досліджень з використанням розглянутих в курсі формальних методів розробки та верифікації інформаційно-керуючих систем. Вміє використовувати сучасні інформаційні технології для проведення наукових досліджень з формальних методів розробки та верифікації інформаційно-керуючих систем.

Відмінно (90-100). Здати обидва модулі з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати. Опублікувати наукову статтю (у співавторстві) за тематикою дисертаційних досліджень з використанням розглянутих в курсі методів розробки та верифікації інформаційно-керуючих систем у науковому журналі, зазначеного у переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора технічних наук та доктора філософії, або у закордонному фаховому журналі, що розміщений у базах цитування IEEEXplore, Scopus, Web of Science.

Шкала оцінювання: бальна і традиційна

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

13. Методичне забезпечення

1. Ілляшенко, О.О., Брежнєв, Е.В., Орєхова, А.О.: Основи ІТ-інженерії безпеки критичних інфраструктур. Національний аерокосмічний університет «Харківський авіаційний інститут», с. 185. Харків (2013)
2. Ілляшенко, О.О., Харченко, В.С., Чуйков, Я.О.: Оцінка безпеки систем на FPGA з використанням XMECA для V-моделі життєвого циклу. Радіоелектронні и комп'ютерні системи, № 6 (80), с. 141-179 (2016)

14. Рекомендована література

Базова:

1. 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)
2. 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)
3. 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)
4. 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)
5. Illiashenko, O., Potii, O., Komin, D.: Advanced security assurance case based on ISO/IEC 15408. In: Theory and Engineering of Complex Systems зфтand 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)
6. 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.

Допоміжна:

1. Bishop, P., Bloomfield, R., Guerra, S.: The future of goal-based assurance cases. In: Proceedings of Workshop on Assurance Cases. Supplemental Volume of the 2004 International Conference on Dependable Systems and Networks, pp. 390–395, Florence, Italy, June 2004
2. ASCAD – Adelard safety case development manual. In: Adelard. (2010)
3. Draft GSN Standard, version 1.0. In: York University (2010)

4. Cyra, Ł.: A method of trust case templates to support standards conformity achievement and assessment. (2008)

5. Górski, J., Cyra, Ł., Jarzębowicz, A., Miler, J.: Argument strategies and patterns of the trust-IT framework. In: Polish Journal of Environmental Studies, vol.17 no. 4C, pp.323-329. Poland (2008)

6. National Defense Industrial Association (NDIA) system assurance committee. Engineering for System Assurance. In: Arlington, VA: NDIA. (2008)

7. The purpose, scope, and content of safety cases, ONR nuclear safety technical assessment guide, http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-051.pdf (2015).

8. Adelard safety case development manual, http://www.adelard.com/resources/ascad/ascad_download.html (2015)

9. The Adelard Safety Case Editor – ASCE. In: Adelard. https://www.adelard.com/asce/choosing-asce/index/ (2010)

10. Guerra, S., Bishop, P., Bloomfield, R., Sheridan, D.: Assessment and qualification of smart sensors. In: Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies: proceedings of 7th International Topical Meeting 7-11 November 2010. – Las Vegas, pp. 499 – 510 (2010)

11. Nobes, T. S.: Smart instruments in safety instrumented systems. In: InTech, Vol.56, №.7, pp. 14 – 19 (2009)

12. COBRA - security risk analysis & assessment. http://www.riskworld.net/ (2018)

13. Condor - A system for developing and managing information security policies. Digital Security http://www.dsec.ru/products/kondor/ (2018)

14. SESAMO. Security and safety modelling. http://sesamo-project.eu. (2018)

Стандарти

1. 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)

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

3. ДСТУ ISO/IEC 15408-2:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги (ISO/IEC 15408-2:2008, IDT)

4. ДСТУ ISO/IEC 15408-3:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 3. Вимоги до гарантії безпеки (ISO/IEC 15408-3:2008, IDT)

5. ДСТУ ISO/IEC 18045:2015 Інформаційні технології. Методи захисту. Методологія оцінювання безпеки IT (ISO/IEC 18045:2008, IDT)

6. ISO/IEC 15443-1:2012: International Organization for Standardization. International Electrotechnical Commission. Information technology – Security techniques.

7. 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.

8. 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.

9. ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT).

10. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБ України. Київ, Україна (1999). Із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806.

11. НД ТЗІ 2.7-009-09: Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу. ДСТСЗІ СБ України. Київ, Україна (2009). Із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806.

12. НД ТЗІ 2.7-010-09: Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу. ДСТСЗІ СБ України. Київ, Україна.

13. НД ТЗІ 2.6-001-11: Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. ДСТСЗІ СБ України. Київ, Україна (2011). Із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806.

15. Інформаційні ресурси

1. https://ieeexplore.ieee.org/Xplore/home.jsp
2. https://www.scopus.com/search/form.uri?display=basic
3. https://mjl.clarivate.com/search-results