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

Теорія і методи безпеки індустріальних систем
(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

Теорія і методи безпеки індустріальних систем
(назва дисципліни)

для здобувачів за спеціальністю 125 "Кібербезпека"

освітньо-наукової програми "Кібербезпека"

«26» 08 2020 р., – 15 с.

Розробник: професор, д.т.н., професор _____ Скляр В.В.
(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 – 2</td><td rowspan="2">Навчальний рік
2020/2021</td></tr>
<tr><td>Кількість змістовних модулів – 4</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="3">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></td><td>Самостійна робота
82 год.</td></tr>
<tr><td></td><td>Індивідуальні завдання: 0 год.</td></tr>
<tr><td></td><td></td><td>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: формування знань, вмінь та навичок, необхідних для вирішення завдань, пов'язаних із забезпеченням безпеки індустріальних систем з урахуванням сучасних вимог та технологічних рішень, а також, з оцінюванням різних видів безпеки, можливих ризиків, що можуть виникати в процесі експлуатації індустріальних систем, та з розробленням стратегії їх модернізації.

2. Завдання: підготовка фахівців, які володіють базовими поняттями з функціональної безпеки, вміють ефективно управляти функціональною безпекою та життєвим циклом, оцінювати показники функціональної безпеки та організовувати заходи із забезпечення функціональної безпеки.

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 виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у кібербезпеці та дотичних до неї (нього, них) міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з кібербезпеки та суміжних галузей;
- здатність виявляти, ставити та вирішувати проблеми дослідницького характеру в сфері кібербезпеки;
- здатність ініціювати, розробляти і реалізовувати комплексні інноваційні проекти в кібербезпеці та дотичні до неї міждисциплінарні проекти, лідерство під час їх реалізації;
- здатність дотримуватись етики досліджень, а також правил академічної доброчесності в наукових дослідженнях та науково-педагогічній діяльності.

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

- мати передові концептуальні та методологічні знання з кібербезпеки і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з відповідного напряму, отримання нових знань та/або здійснення інновацій;
- вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми кібербезпеки державною та іноземною мовами, кваліфіковано відображати результати досліджень у наукових публікаціях у провідних міжнародних наукових виданнях;
- 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;

- 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;

- розробляти та реалізовувати наукові та/або інноваційні інженерні проєкти, які дають можливість переосмислити наявне та створити нове цілісне знання та/або професійну практику і розв'язувати значущі наукові та технологічні проблеми кібербезпеки з дотриманням норм академічної етики і врахуванням соціальних, економічних, екологічних та правових аспектів;

- уміти управляти змістом, розкладом, вартістю, якістю, ризиками, людськими ресурсами та комунікаціями науково-технічних проектів в аерокосмічній галузі з відповідністю вимогам міжнародних стандартів.

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», «Теорія планування експерименту».

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

3. Програма навчальної дисципліни

Модуль 1. Основи аналізу безпеки

Змістовний модуль 1. *Базові поняття безпеки.*

ТЕМА 1. Предмет, мета вивчення і задачі дисципліни.

Предмет, мета вивчення і задачі дисципліни. Структура і зміст дисципліни, а також методичні рекомендації по її вивченню. Місце дисципліни в навчальному процесі. Вимоги до знань і умінь студентів. Характеристика рекомендованих під час вивчення дисципліни джерел інформації.

ТЕМА 2. Загальні відомості про безпеку індустріальних систем.

Тенденції розвитку індустріальних систем у контексті глобальної ініціативи «Індустрія 4.0».

Архітектура існуючих індустріальних систем: «Інтернет речей», автоматизовані системи управління технологічними процесами (АСУ ТП), вбудовані системи, програмовані логічні контролери (ПЛК).

Головні риси, які відрізняють сучасні індустріальні системи («Індустрія 4.0») від систем попередніх поколінь. Приклади програмно-технічних рішень.

Задачі забезпечення інформаційної та функціональної безпеки при зрощенні технологій «Інтернет речей» та АСУ ТП. Ризики експлуатації індустріальних систем. Джерела ризиків та приклади порушень безпеки.

Властивості індустріальних систем. Головні атрибути інформаційної та функціональної безпеки. Структура вимог до інформаційної та функціональної безпеки.

Структура вивчення навчальної дисципліни "Теорія і методи безпеки індустріальних систем". Структура Assurance Case, як збірника артефактів оцінювання та забезпечення безпеки.

ТЕМА 3. Вимоги стандартів щодо безпеки індустріальних систем.

Огляд стандартів з інформаційної та функціональної безпеки індустріальних систем.

Стандарт IEC 61508-1:2010 Functional safety of electrical/electronic/ programmable electronic safety-related systems (далі - IEC 61508) . Зв'язки між частинами IEC 61508 та короткий зміст частин.

Систематизація вимог до інформаційної та функціональної безпеки. Приклади успішної сертифікації контролерів щодо вимог IEC 61508.

Змістовний модуль 2. ***Керування та оцінювання безпеки.***

ТЕМА 1. Менеджмент інформаційної та функціональної безпеки.

Порівняння менеджменту інформаційної та функціональної безпеки. План керування функціональною безпекою та його зв'язок з системою менеджменту інформаційної безпеки.

План керування персоналом. План керування конфігурацією. Керування змінеммями. Вибір та оцінювання програмних засобів розробки. План верифікації та валідації. План документування та структура документів з безпеки.

Оцінювання та аудит інформаційної та функціональної безпеки.

ТЕМА 2. Життєвий цикл інформаційної та функціональної безпеки.

Поняття життєвого циклу. Повний життєвий цикл та життєвий цикл розробки. V-образний життєвий цикл.

Етап «Концепція». Етап «Вимоги». Етап «Архітектурний проект». Етап «Проект програмного забезпечення». Етап «Проект технічних засобів». Етап «Кодування програмного забезпечення».

Етап «Тестування програмного забезпечення». Етап «Інтеграційне тестування». Етап «Валідація». Етап «Введення до експлуатацій». Етап «Експлуатація та супроводження». Етап «Зняття з експлуатації».

Планування життєвого циклу.

ТЕМА 3. Оцінювання функціональної безпеки.

Структура атрибутів інформаційної та функціональної безпеки. Підхід до аналізу ризиків індустріальних систем та встановлення рівнів інтегрованості функціональної безпеки.

Зв'язок показників надійності та функціональної безпеки. Інтенсивності безпечних та небезпечних, діагностовних та недіагностовних відмов. Середня імовірність небезпечної відмови за запитом функції безпеки. Середня частота

небезпечних відмов функції безпеки. Доля безпечних відмов. Діагностичне покриття.

Вимоги до кількісних показників функціональної безпеки ІУС згідно IEC 61508. Методологія аналізу видів, режимів та критичності відмов (FMECA). Оптимізація структури ІУС за показниками готовності та критерієм функціональної безпеки.

Модуль 2. Основи забезпечення безпеки

Змістовний модуль 1. ***Огляд підходів до забезпечення безпеки індустріальних систем.***

ТЕМА 1. Методи забезпечення функціональної безпеки індустріальних систем.

Топологічні та конструктивні особливості індустріальних систем. Типові програмно-апаратні рішення із забезпечення функціональної безпеки індустріальних систем.

Багатоканальні архітектури. Резервування комп'ютерної мережі. Резервування електроживлення. Захист від падіння та підвищення напруги електроживлення. Принцип незалежності та фізичне і логічне розділення компонентів.

Самодіагностування. Контроль конфігурації апаратно-програмних засобів. Контроль часових параметрів функціонування програмного забезпечення. Сторожовий таймер. Контроль точності та діагностування аналогових входів та виходів. Автоматичний перехід вихідних сигналів у безпечній стан. Контроль комунікацій та циклічні коди (CRC).

Захист від зовнішніх впливів: вентиляція та контроль температури, екранування та фізичне розподілення кабелів, вібростійкість, корозостійкість, захист від вологи та пилу.

Використання якісних компонентів. Принцип діверсності.

Типові організаційні заходи із забезпечення функціональної безпеки індустріальних систем. Управління проектами.

Формальні та полуформальні нотації для розробки специфікації вимог та проектів індустріальних систем та програмних і апаратних компонентів. Структурований процес розробки системи та програмного забезпечення. Використання кращих практик та стандартів безпечного програмування.

Використання сертифікованих компіляторів та трансляторів коду та сертифікованих бібліотек програмних компонентів.

Виконання всебічних оглядів, аналізу та тестування при верифікації та валідації. Контроль якості при виробництві апаратних компонентів.

Ергономічний людино-машинний інтерфейс та захист від помилок оператора. Підтримка захисту від несанкціонованого доступу. Супроводження при експлуатації та врахування опиту експлуатації.

ТЕМА 2. Особливості забезпечення інформаційної безпеки індустріальних систем.

Огляд стандартів з інформаційної безпеки індустріальних систем.

Порівняльний аналіз властивостей індустріальних та інформаційних систем.

Структура гармонізованих вимог до інформаційної та функціональної безпеки індустріальних систем.

Оцінювання ризиків та управління ризиками. Організація управління безпекою за тріадою «Персонал – Процеси – Технології».

Контекст вимог до індустріальних систем та моделі індустріальних систем. Концепція рівнів інформаційної безпеки та зонування обладнання індустріальних систем.

Змістовний модуль 2. ***Застосування методології Assurance Case з врахуванням вимог до функціональної та інформаційної безпеки.***

ТЕМА 1. Управління вимогами до безпеки.

Процес інженерії вимог. Ідентифікація та аналіз вимог. Верифікація і валідація вимог. Забезпечення якості вимог. Пряме та зворотне трасування вимог. Програмні засоби підтримки трасування вимог.

ТЕМА 2. Методи тестування індустріальних систем.

Організація процесу верифікації та вилідації індустріальних систем та її програмно-апаратних компонентів.

Огляд специфікації вимог. Огляд специфікації архітектурного проекту. Огляд проекту апаратних засобів.

Аналіз надійності та аналіз видів, режимів та критичності відмов (FMECA).

Огляд проекту програмного забезпечення. Огляд та статичний аналіз програмного коду. Тестування програмного коду.

Особливості верифікації та валідації індустріальних систем на базі програмованих логічних інтегральних схем (ПЛІС).

Тестування із засівом дефектів. Інтеграційне тестування. Валідаційне тестування. Тестування на стійкість до зовнішніх впливів.

ТЕМА 3. Методологія Assurance Case.

Зміст та теоретичні основи методології Assurance Case. Формальна нотація CAE (Claim – Argument – Evidence). Формальна нотація GSN (Goal Structured Notation). Інтеграція методології Assurance Case у життєвий цикл індустріальних систем. Програмні засоби підтримки методології Assurance Case.

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	7
Модуль 1					
Змістовний модуль 1. *Базові поняття безпеки.*					
Тема 1. Предмет, мета вивчення і задачі дисципліни.	1	1			
Тема 2. Загальні відомості про безпеку індустріальних систем.	16	3		4	9
Тема 3. Вимоги стандартів щодо безпеки індустріальних систем.	13	2		2	9
Разом за змістовним модулем 1	30	6		6	18
Змістовний модуль 2. *Керування та оцінювання безпеки.*					
Тема 1. Менеджмент інформаційної та функціональної безпеки	15	4		2	9
Тема 2. Життєвий цикл інформаційної та функціональної безпеки.	15	4		4	7
Тема 3. Оцінювання функціональної безпеки.	15	4		4	7
Разом за змістовним модулем 2	45	12		10	23
Разом за модулем 2	**75**	**18**		**16**	**41**
Модуль 2					
Змістовний модуль 1. *Огляд підходів до забезпечення безпеки індустріальних систем.*					
Тема 1. Методи забезпечення функціональної безпеки індустріальних систем.	17	4		4	9
Тема 2. Особливості забезпечення інформаційної безпеки індустріальних систем.	13	2		2	9
Разом за змістовним модулем 1	30	6		6	18
Змістовний модуль 2. *Застосування методології Assurance Case з врахуванням вимог до функціональної та інформаційної безпеки.*					
Тема 1. Управління вимогами до безпеки.	15	2		4	9
Тема 2. Методи тестування індустріальних систем.	15	4		4	7
Тема 3. Методологія Assurance Case.	15	4		4	7
Разом за змістовним модулем 2	45	10		12	23
Разом за модулем 2	**75**	**16**		**18**	**41**
Усього годин	**150**	**34**		**34**	**82**

5. Теми семінарських занять

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

6. Теми практичних занять

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

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Аналіз програмно-апаратних продуктів, сертифікованих на відповідність вимогам до функціональної безпеки	4
2	Аналіз вимог стандартів у галузі безпеки індустріальних систем	2
3	Складання плану керування функціональною безпекою	2
4	Розробка структури життєвого циклу безпеки	4
5	Оцінювання показників безпеки	4
6	Аналіз та вибір засобів забезпечення функціональної безпеки	4
7	Аналіз та вибір засобів забезпечення інформаційної безпеки	2
8	Трасування вимог	4
9	Розробка тестової документації	4
10	Використання програмних засобів підтримки методології Assurance Case	4
	Разом	**34**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Властивості сучасних ІУС за версією National Institute of Standards and Technologies (на прикладі документу NIST SP 800-82, Guide to Industrial Control Systems Security)	9
2	Зміст стандартів серіі IEC 61508	9
3	Звід знань щодо менеджменту проектів (PMBOK) у частині керування персоналом та керування конфігураціями	9
4	Життєвий цикл критичного програмного забезпечення (згідно IEC 61508-3)	7

№ з/п	Назва теми	Кількість годин
5	Розрахунок показників надійності систем безпеки (згідно ABB Safety Handbook)	7
6	Методи за заходи захисту від випадкових та систематичних відмов (згідно IEC 61508-7)	9
7	Глосарій термінів та сіллабус щодо підготовки професіоналів з інженерії вимог	9
8	Глосарій термінов та сілабус щодо підготовки професіоналів з тестування	9
9	Зміст стандартів серіі IEC 62443	7
10	Стандарт з нотації GSN (Structured Goal Notation)	7
	Разом	**82**

9. Індивідуальні завдання

Не передбачено

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 екзамену.

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
Модуль 1			
Робота на лекціях	0…1	5	0…5
Виконання лабораторних робіт	0…5	2	0...10
Модульний контроль	0…10	1	0…10
Модуль 2			
Робота на лекціях	0…1	5	0…5
Виконання лабораторних робіт	0…5	2	0…10
Написання і рецензування статей	0…25	2	0…50
Модульний контроль	0…10	1	0…10
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:

– базові поняття з безпеки;

– міжнародними стандарти в сфері функціональної, інформаційної та кібербезпеки;

– основи управління безпекою та життєвим циклом індустріальних систем;

– основи кількісного оцінювання функціональної безпеки та розрахунку показників функціональної безпеки;

– основи технічних та організаційних заходів забезпечення безпеки.

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 забезпечення безпеки індустріальних систем.

12.3 Критерії оцінювання роботи студента протягом семестру

Задовільно (60-74). Знати базові поняття, що стосуються функціональної, інформаційної та кібербезпеки. Виконати рецензування двох статей: україномовної та англомовної.

Добре (75-89). Мати достатньо глибоке знання програмного матеріалу, володіти понятійним апаратом, вміти аргументувати свої відповіді, але у відповідях допускаються неточності. Відвідати і виконати не менше 90% лабораторних робіт. Отримати з редакції наукового журналу, зазначеного у переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукового ступеня доктора філософії, підтвердження про прийняття до публікації наукової статті (у співавторстві) за тематикою дисертаційних досліджень з використанням розглянутих в курсі методів та засобів забезпечення безпеки індустріальних систем. Уміти використовувати сучасні інформаційні технології для проведення наукових досліджень із забезпечення та оцінювання безпеки індустріальних 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 та засобів забезпечення безпеки індустріальних 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 і 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

Скляр, В.В. Забезпечення безпеки АСУТП відповідно до сучасних стандартів [Текст] / В.В. Скляр. - М .: Инфра-Інженерія, 2018, 384 с.

14. Рекомендована література

Базова:

1. Федоров, Ю.Н. Довідник інженера по АСУ ТП: Проектування і розробка [Текст] / Ю.М. Федоров. - М .: Инфра-Інженерія, 2008. - 928 с.

2. Leveson, N. Engineering a Safer World: Systems Thinking Applied to Safety [Text] / N. Leveson. – The MIT Press, 2011. – 534 p.

3. Smith, D. Functional Safety. A Straightforward Guide to applying IEC 61508 and Related Standards [Text] / D. Smith, K. Simpson. – Elsevier Butterworth-Heinemann, Oxford, UK, 2004. – 263 p.

4. Medoff, M. Functional Safety – An IEC 61508 SIL 3 Compatible Development Process [Text] / M. Medoff, R. Faller. – exida.com L.L.C., Sellersville, PA, USA, 2010. – 281 p.

5. Basilio, A. Functional Safety of Safety–Related Systems. Manual for Plant Engineering and Maintenance [Text] / A. Basilio, F. Landrini, G. Novelli, G. Landrini, M. Baldrigh]. – G.M. International S.r.l, Villasanta, Italy, 2008. – 388 p

Допоміжна:

1. Тюрін, О.Г. Управління потенційно небезпечними технологіями [Текст] / О.Г. Тюрін, В.С. Кальницький, Е.Ф. Жегров. - М .: Инфра-Інженерія, 2011, 288 с.

2. NIST SP 800-82 Revision 2, Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC). – National Institute of Standards and Technologies, 2015.

3. Керівництво до зводу знань з управління проектами (Керівництво PMBOK®), П'яте видання. - Project Management Institute, Inc., 2013.

4. ABB Safety Handbook. Machine Safety – Jokab Safety products. – ABB, 2013.

5. Syllabus: REQB® Certified Professional for Requirements Engineering. Foundation Level, Version 2.1. – Requirements Engineering Qualification Board, 2014.

6. Standard glossary of terms used in Requirements Engineering, Version 1.3. – Requirements Engineering Qualification Board, 2014.

7. Certified Tester Foundation Level Syllabus. – International Software Testing Qualifications Board, 2011.

8. Standard glossary of terms used in Software Testing, Version 2.3. – International Software Testing Qualifications Board, 2014.

9. GSN Community Standard ,Version 1. – Origin Consulting (York) Limited, 2011.

Стандарти

1. IEC 61508-1:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements.

2. IEC 62443-2-1 Ed. 1.0 b:2010, First Edition: Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program

3. IEC 62443-3-3:2013 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels.

15. Інформаційні ресурси

1. Video lectures "Functional Safety of Computer Systems"
2. Slides of lectures
3. Vladimir Sklyar blog at habr.com
4. http://csrc.nist.gov/publications/
5. https://habr.com/ru/hub/infosecurity/