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

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

ЗАТВЕРДЖУЮ
Голова НМК
_____ М.С. Зряхов
(підпис) (ініціали та прізвище)
«30» 08 2019 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Технології розроблення та забезпечення функціональної безпеки ІУС
(назва навчальної дисципліни)

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

Спеціальність: 125 "Кібербезпека"
(код та найменування спеціальності)

Освітня програма: Безпека інформаційних і комунікаційних систем
Освітні програма: Кібербезпека індустріальних систем
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: другий (магістерський)

Харків 2019 рік

Робоча програма Технології розроблення та забезпечення функціональної безпеки ІУС
(назва дисципліни)

для студентів за спеціальністю: 125 "Кібербезпека"
(код та найменування спеціальності)

Освітня програма: Безпека інформаційних і комунікаційних систем
(найменування освітньої програми)

Освітні програма: Кібербезпека індустріальних систем
(найменування освітньої програми)

«26» 08 2019 р., – 14 с.

Розробник: Скляр В.В., професор, д.т.н., професор
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол №1 від «30» 08 2019 р.

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

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 – 7,5</td><td rowspan="11">Галузь знань:
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність:
125 "Кібербезпека"

Освітні програми:
"Безпека інформаційних і комунікаційних систем"
"Кібербезпека індустріальних систем"

Рівень вищої освіти:
другий (магістерський)</td><td>Цикл загальної підготовки: нормативна</td></tr>
<tr><td>Кількість модулів – 2</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістовних модулів – 4</td><td>2019/ 2020</td></tr>
<tr><td>Індивідуальне завдання
(назва)</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 64/225</td><td>9-й</td></tr>
<tr><td>Лекції *</td></tr>
<tr><td rowspan="2">Тижневих годин для денної форми навчання: аудиторних – 4 самостійної роботи студента – 5</td><td>32 години</td></tr>
<tr><td>Практичні, семінарські*</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Лабораторні *</td></tr>
<tr><td>32 години</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>161 години</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: *64/161.*

* Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета вивчення: (ВБ1.5) підготовка студентів до вирішення завдань пов'язаних з забезпеченням безпеки вбудованих систем та засобів, що формують IoT інфраструктуру.

Завдання: (Б1.5) придбання студентами необхідних знань та вмінь в сфері розроблення безпечної IoT інфраструктури з урахуванням сучасних вимог та технологічних рішень; формування у студентів навичок оцінювання різних видів безпеки, можливих ризиків, що можуть виникати в процесі експлуатації IoT систем та розроблення стратегії їх модернізації, а також:

– придбання знань про базові поняття з функціональної безпеки;

– придбання знань про основи управління функціональною безпекою та життєвим циклом ІУС;

– придбання знань про основи кількісного оцінювання функціональної безпеки та розрахунку показників функціональної безпеки;

– придбання знань про основи технічних та організаційних заходів забезпечення функціональної безпеки.

Програмні компетентності. Дисципліна має допомогти сформувати у студентів такі компетентності

– (ЗК1) здатність до абстрактного мислення, аналізу та синтезу;

– (ЗК2) здатність застосовувати знання у практичних ситуаціях;

– (ЗК3) здатність планувати та управляти часом;

– (ЗК4) навички використання інформаційних і комунікаційних технологій;

– (ЗК5) здатність до пошуку, оброблення та аналізу інформації з різних джерел;

– (ЗК6) здатність бути критичним і самокритичним;

– (ЗК7) здатність генерувати нові ідеї (креативність);

– (ЗК8) здатність приймати обґрунтовані рішення;

– (ЗК10) здатність розробляти та управляти проектами;

– (ЗК11) прихильність безпеці;

– (ЗК12) здатність оцінювати та забезпечувати якість виконуваних робіт;

– (ЗК13) визначеність і наполегливість щодо поставлених завдань і взятих обов’язків;

– (ФК2) базові знання фундаментальних наук в обсязі, необхідному для освоєння загально професійних дисциплін;

– (ФК3) вміння виявляти, аналізувати та вирішувати проблеми у професійній сфері;

– (ФК5) здатність до участі у проектній діяльності; здатність до адаптації та дії в новій ситуації;

– (ФК6) володіння науковими методами обґрунтування, вибору та аналізу криптографічних механізмів і систем захисту;

– (ФК10) здатність виконувати роботи з проектування складних комплексів засобів захисту та управління функціональною безпекою інформаційно-управляючих систем відповідно до сфери їх застосування;

– (ФК11) здатність здійснювати та детально обґрунтовувати вибір структури, принципів організації, комплексів засобів і технологій забезпечення безпеки систем та мереж;

– (ФК12) здатність аналізувати та здійснювати обґрунтований вибір технологій і засобів розробки кібербезпечних апаратних комплексів та систем, що програмуються.

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

– (ПРН1) уміти грамотно висловлюватися в усній та писемній формі;

– (ПРН2) здатність використовувати мову професійного спілкування;

– (ПРН4) вміти аргументувати свої думки;

– (ПРН5) вміти аналізувати матеріал і робити висновки;

– (ПРН6) пошук інформації в різних джерелах для розв’язання задач спеціальності;

– (ПРН7) здатність продемонструвати розуміння впливу рішень у суспільному і соціальному контексті;

– (ПРН8) розуміти й інтерпретувати вивчене;

– (ПРН9) використовувати вивчений матеріал у нових ситуаціях;

– (ПРН17) здійснювати вибір методів і засобів для побудови безпечних розподілених систем.

Крім того, студенти повинні бути здатні проводити роботу щодо оцінювання та забезпечення функціональної безпеки ІУС

Міждисциплінарні зв’язки. Дисципліна базується на знаннях, отриманих під час вивчення дисциплін у циклі загальної і професійної підготовки, передбачених навчальним планом спеціальності.

Матеріал дисципліни базується на знаннях, отриманих під час вивчення дисциплін із циклу загальної підготовки, зокрема "Вища математика", "Фізика", "Теорія електричних кіл і мікроелектроніка", "Іноземна мова".

Матеріал дисципліни базується на знаннях, отриманих під час вивчення дисциплін із циклу професійної підготовки, а саме "Основи функціонування комп'ютерів", "Технології програмування", "Дискретна математика".

Матеріал, засвоєний під час вивчення цієї дисципліни, є базою для дисциплін із циклу професійної підготовки, а саме "Методи та технології кібербезпеки критичних інфраструктур".

3. Програма навчальної дисципліни

Модуль 1. Основи аналізу функціональної безпеки
Змістовний модуль 1. ***Базові поняття функціональної 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 функціональну безпеку ІУС.
Тенденції розвитку ІУС у контексті глобальної ініціативи «Індустрія 4.0». Архітектура існуючих ІУС: «Інтернет речей», автоматизовані системи управління технологічними процесами (АСУ ТП), вбудовані системи, програмовані логічні контролери (ПЛК).
Задачі забезпечення інформаційної та функціональної безпеки при зрощенні технологій «Інтернет речей» та АСУ ТП.
Ризики експлуатації ІУС. Джерела ризиків та приклади порушень функціональної безпеки.
Властивості ІУС. Головні атрибути інформаційної та функціональної безпеки. Структура вимог до інформаційної та функціональної безпеки.
Структура вивчення навчальної дисципліни "Технології розроблення та забезпечення функціональної безпеки ІУС". Структура Assurance Case, як збірника артефактів оцінювання та забезпечення функціональної безпеки.
ТЕМА 3. Вимоги стандартів щодо функціональної безпеки ІУС.
Огляд стандартів з інформаційної та функціональної безпеки ІУС.
Стандарт МЕК 61508 «Функціональна безпека систем електричних, електронних, програмованих електронних, пов'язаних з безпекою». Зв'язки між частинами МЕК 61508 та короткий зміст частин.
Систематизація вимог до інформаційної та функціональної безпеки. Приклади успішної сертифікації контролерів щодо вимог МЕК 61508.

Змістовний модуль 2. ***Керування та оцінювання функціональної безпеки*****.**
ТЕМА 1. Менеджмент функціональної безпеки.
Порівняння менеджменту інформаційної та функціональної безпеки. План керування функціональною безпекою.
План керування персоналом. План керування конфігурацією. Керування змінеммами. Вибір та оцінювання програмних засобів розробки. План верифікації та валідації. План документування та структура документів з функціональної безпеки.
Оцінювання та аудит 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 ІУС 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 функціональної безпеки

Змістовний модуль 1. ***Огляд підходів до забезпечення функціональної безпеки ІУС*****.**

ТЕМА 1. Методи забезпечення функціональної безпеки ІУС.

Топологічні та конструктивні особливості ІУС. Типові програмно-апаратні рішення із забезпечення функціональної безпеки ІУС.
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 ІУС. Управління проектами.
Формальні та полуформальні нотації для розробки специфікації вимог та проектів ІУС 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. Управління вимогами до функціональної 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 3. Методи тестування ІУС.
Організація процесу верифікації та вилідації ІУС 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 ІУС на базі програмованих логічних інтегральних схем (ПЛІС).
Тестування із засівом дефектів. Інтеграційне тестування. Валідаційне тестування. Тестування на стійкість до зовнішніх впливів.

Змістовний модуль 2. ***Застосування методології Assurance Case з врахуванням вимог до функціональної та інформаційної безпеки*****.**
ТЕМА 1. Забезпечення інформаційної безпеки ІУС.
Огляд стандартів з інформаційної безпеки ІУС. Порівняльний аналіз властивостей ІУС та інформаційних систем.
Структура гармонізованих вимог до інформаційної та функціональної безпеки ІУС. Оцінювання ризиків та управління ризиками. Організація управління безпекою за тріадою «Персонал – Процеси – Технології».
Контекст вимог до АСУ ТП та моделі АСУ ТП. Концепція рівнів інформаційної безпеки та зонування обладнання АСУ ТП.
ТЕМА 2. 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 ІУС. 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 функціональної безпеки*.					
Тема 1. Предмет, мета вивчення і задачі дисципліни.	1	1		-	-
Тема 2. Загальні відомості про функціональну безпеку ІУС.	23	1		2	20
Тема 3. Вимоги стандартів щодо функціональної безпеки ІУС. Модульний контроль	28	4		4	20
Разом за змістовним модулем 1	**52**	**6**		**6**	**40**
Змістовний модуль 2. *Керування та оцінювання функціональної безпеки*.					
Тема 1. Менеджмент функціональної безпеки.	22	4		4	14
Тема 2. Життєвий цикл інформаційної та функціональної безпеки.	19	4		2	13
Тема 3. Оцінювання функціональної безпеки. Модульний контроль	19	2		4	13
Разом за змістовним модулем 2	**60**	**10**		**10**	**40**
Усього годин за модулем 1	**112**	**16**		**16**	**80**
Модуль 2					
Змістовний модуль 1. *Огляд підходів до забезпечення функціональної безпеки ІУС*.					
Тема 1. Методи забезпечення функціональної безпеки ІУС.	22	4		4	14
Тема 2. Управління вимогами до функціональної безпеки.	17	2		2	13
Тема 3. Методи тестування ІУС. Модульний контроль	21	4		4	13
Разом за змістовим модулем 1	**60**	**10**		**10**	**40**
Змістовний модуль 2. *Застосування методології Assurance Case з врахуванням вимог до функціональної та інформаційної безпеки*.					
Тема 1. Забезпечення інформаційної безпеки ІУС.	27	4		2	21
Тема 2. Методологія Assurance Case Модульний контроль	26	2		4	20
Разом за змістовним модулем 2	**53**	**6**		**6**	**41**
Усього годин за модулем 2	**113**	**16**		**16**	**81**
Усього годин	**225**	**32**		**32**	**161**

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1		
	Разом	

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1		
	Разом	

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	Аналіз програмно-апаратних продуктів, сертифікованих на відповідність вимогам до функціональної безпеки	2
2	Аналіз вимог стандартів у галузі безпеки індустріальних систем	4
3	Складання плану керування функціональною безпекою	4
4	Розробка структури життєвого циклу безпеки	2
5	Оцінювання показників безпеки	4
6	Аналіз та вибір засобів забезпечення функціональної безпеки	4
7	Трасування вимого до безпеки	2
8	Розробка тестової документації	4
9	Аналіз та вибір засобів забезпечення інформаційної безпеки	2
10	Використання програмних засобів підтримки методології Assurance Case	4
	Разом	**32**

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)	20
2	Зміст стандартів серії МЕК 61508	20

№ з/п	Назва теми	Кількість годин
3	Звід знань щодо менеджменту проектів (PMBOK) у частині керування персоналом та керування конфігураціями	14
4	Життєвий цикл критичного програмного забезпечення (згідно МЕК 61508-3)	13
5	Розрахунок показників надійності систем безпеки (згідно ABB Safety Handbook)	13
6	Методи за заходи захисту від випадкових та систематичних відмов (згідно МЕК 61508-7)	14
7	Глосарій термінів та сіллабус щодо підготовки професіоналів з інженерії вимог	13
8	Глосарій термінов та сілабус щодо підготовки професіоналів з тестування	13
9	Зміст стандартів серії МЕК 62443	21
10	Стандарт з нотації GSN (Structured Goal Notation)	20
	Разом	**161**

9. Індивідуальні завдання

Не передбачено навчальним планом

10. Методи навчання

Проведення аудиторних лекцій, практичних занять, консультацій, а також самостійна робота студентів за відповідними матеріалами (п.10, 11).

11. Методи контролю

Проведення поточного контролю, підсумковий контроль у вигляді іспиту.

12. Критерії оцінювання та розподіл балів, які отримують студенти

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

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Модуль 1			
Виконання і захист лабораторних робіт	0...5	3	0…15
Тестування знань	0...5	3	0...15
Модульний контроль	0…15	1	0…15
Модуль 2			
Виконання і захист лабораторних робіт	0...5	4	0…20
Тестування знань	0...5	4	0...20
Модульний контроль	0…15	1	0…15
Усього за семестр			**0…100**

Семестровий контроль у вигляді іспиту за наявності допуску до іспиту. Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Білет для іспиту складається з одного теоретичного та одного практичного запитань, максимальна кількість за кожне із запитань, складає 50 балів.

12.2. Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки:

– знати базові поняття з функціональної безпеки, основи управління функціональною безпекою та життєвим циклом ІУС.

Необхідний обсяг вмінь для одержання позитивної оцінки:

– вміти використовувати нормативні документи, вітчизняні та міжнародні стандарти щодо вимог з функціональної безпеки;

– вміти проводити кількісне оцінювання функціональної безпеки;

– вміти впроваджувати технічні та організаційні заходи забезпечення функціональної безпеки.

12.3 Критерії оцінювання роботи студента протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Захистити не менше 80% від усіх завдань лабораторних занять. Уміти використовувати нормативні документи, вітчизняні та міжнародні стандарти щодо вимог з функціональної безпеки.

Добре (75-89). Твердо знати необхідний обсяг знань для одержання позитивної оцінки, захистити не менше 90% завдань лабораторних занять. Уміти використовувати сучасні методи теоретичних та експериментальних досліджень для організації та проведення робіт щодо оцінювання та забезпечення функціональної безпеки. Мати необхідний обсяг вмінь для одержання позитивної оцінки.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати. Уміти виконувати заходи щодо забезпечення функціональної безпеки.

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. Скляр В.В. Конспект лекцій з дисципліни «Технології розроблення та забезпечення функціональної безпеки ІУС».

2. Скляр В.В. Методичні вказівки щодо виконання лабораторних робот з дисципліни «Технології розроблення та забезпечення функціональної безпеки ІУС».

14. Рекомендована література

Базова

1. Федоров, Ю.Н. Справочник инженера по АСУ ТП: Проектирование и разработка [Текст] / Ю.Н. Федоров. – М.: Инфра–Инженерия, 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
6. Тюрин, О.Г. Управление потенциально опасными технологиями [Текст] / О.Г. Тюрин, В.С. Кальницкий, Е.Ф. Жегров. – М.: Инфра–Инженерия, 2011, 288 с.
7. Скляр, В.В. Обеспечение безопасности АСУТП в соответствии с современніми стандартами [Текст] / В.В. Скляр. – М.: Инфра–Инженерия, 2018, 384 с.

Допоміжна

8. 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.
9. Руководство к своду знаний по управлению проектами (Руководство PMBOK®), Пятое издание. – Project Management Institute, Inc., 2013.
10. ГОСТ Р МЭК 61508, Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью [Электронный ресурс]. – Режим доступа: http://standartgost.ru/.
11. ГОСТ Р МЭК 62443-2-1-2015, Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики [Электронный ресурс] – Режим доступа: http://standartgost.ru/.
12. ГОСТ Р МЭК 62443-3-3-2016, Сети промышленной коммуникации. Безопасность сетей и систем. Часть 3-3. Требования к системной безопасности и уровни безопасности [Электронный ресурс] – Режим доступа: http://standartgost.ru/.
13. ABB Safety Handbook. Machine Safety – Jokab Safety products. – ABB, 2013.

14. Syllabus: REQB® Certified Professional for Requirements Engineering. Foundation Level, Version 2.1. – Requirements Engineering Qualification Board, 2014.
15. Standard glossary of terms used in Requirements Engineering, Version 1.3. – Requirements Engineering Qualification Board, 2014.
16. Certified Tester Foundation Level Syllabus. – International Software Testing Qualifications Board, 2011.
17. Standard glossary of terms used in Software Testing, Version 2.3. – International Software Testing Qualifications Board, 2014.
18. GSN Community Standard ,Version 1. – Origin Consulting (York) Limited, 2011.

15. Інформаційні ресурси

1. Вікіпедія – свобідна енциклопедія [Електрон. ресурс]. – Режим доступу: http://www. ru.wikipedia.org/.
2. Відкрита база ГОСТів [Електрон. ресурс] – Режим доступу: http://standartgost.ru/.
3. Публікації з кібербезпеки National Institute of Standards and Technologies [Електрон. ресурс] – Режим доступу: http://csrc.nist.gov/publications/PubsSPs.html#SP 800/.
4. Електронний ресурс інженерів з інформаційних технологій «Хабрахабр» (хаб «Промислове програмування») [Електрон. ресурс] – Режим доступу: https://habrahabr.ru/hub/industrial_control_system/.
5. Асоціація підприємств промислової автоматизації України (АППАУ) [Електрон. ресурс] – Режим доступу: http://appau.org.ua/.