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

_____ Д.М. Крицький
(підпис) (ініціали та прізвище)

« 31 » серпня 2021 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Надійність і функціональна безпека інформаційно-керуючих систем
(назва навчальної дисципліни)

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

Спеціальність: 123 "Комп'ютерна інженерія"
(код та найменування спеціальності)

Освітня програма: Комп'ютерні системи та мережі
Освітня програма: Системне програмування
Освітня програма: Програмовні мобільні системи та Інтернет речей

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2021 рік

Розробник: Харченко В. С., завідувач кафедри, 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 2021р.

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 – 4,5</td><td rowspan="11">Галузь знань
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність
123 "Комп’ютерна інженерія"
(код та найменування)

Освітня програма
Комп’ютерні системи та мережі
Системне програмування
Програмовні мобільні системи та Інтернет речей
(найменування)

Рівень вищої освіти:

перший (бакалаврський)</td><td>Обов’язкова</td></tr>
<tr><td>Кількість модулів – 2</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістовних модулів – 4</td><td>2021/ 2022</td></tr>
<tr><td>Індивідуальне завдання: 1</td><td>Семестр</td></tr>
<tr><td>Загальна кількість годин:
64 / 135</td><td>7-й</td></tr>
<tr><td rowspan="6">Кількість тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи студента – 4,5</td><td>Лекції [1)]</td></tr>
<tr><td>32 годин</td></tr>
<tr><td>Практичні, семінарські[1)]</td></tr>
<tr><td>8 годин</td></tr>
<tr><td>Лабораторні [1)]</td></tr>
<tr><td>24 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>71 година</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>Модульний контроль, іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: 64/71.

[1)] Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета вивчення: здатність аналізувати надійність та функціональну безпеку типових компонентів та систем кібербезпеки та володіти навичками оцінювання та забезпечення показників надійності та безпеки відповідно до вимог.

Завдання знати основні поняття та показники та вимоги до надійності та функціональної безпеки систем кібербезпеки відповідно до міжнародних і національних стандартів; знати та застосувати методики та засоби аналізу та оцінювання надійності та функціональної безпеки систем кібербезпеки; знати та застосувати методики та засоби підвищення надійності та функціональної безпеки систем кібербезпеки з урахуванням ресурсних обмежень.

Компетентності, які набуваються:

- здатність застосовувати знання у практичних ситуаціях;
- знання та розуміння предметної області та розуміння професії;
- здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово;
- зміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;
- здатність до пошуку, оброблення та аналізу інформації;
- здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки;
- здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки;
- здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах;
- здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки;
- здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження;
- здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.);
- здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Очікувані результати навчання:

- в результаті вивчення дисципліни студенти мають досягти такі програмні результати навчання:

- застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
- організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
- використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
- аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;
- адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;
- критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;
- готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;
- вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;
- реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;
- використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

Пререквізити – матеріал дисципліни базується на знаннях, отриманих під час вивчення дисциплін із циклу професійної підготовки, а саме "Основи функціонування комп'ютерів", "Технології програмування", "Дискретна математика", "Комп'ютерна логіка".

Кореквізити - матеріал, засвоєний під час вивчення цієї дисципліни, є базою для дисциплін із циклу професійної підготовки, а саме "Промислові контролери", "Комп'ютерні мережі", а також курсовому і дипломному проектуванні.

3. Програма навчальної дисципліни

Модуль 1. Основи теорії надійності КС

Змістовний модуль 1. Основні поняття та показники надійності та відмовостійкості КС.

Тема 1. Загальна характеристика дисципліни. Базові поняття теорії надійності та безпеки КС.

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. Стани

(справний, несправний; працездатне, непрацездатний; граничне) і події (несправність, пошкодження, відмова; класифікація відмов, відтворення та ремонт; схема станів і подій-переходів). Властивості (системний аналіз властивостей; надійність та її складові: безвідмовність, ремонтопридатність, довговічність і збереженість; відмовостійкість і готовність; живучість і безпека). Системи і елементи в теорії надійності і безпеки (поняття системи і елемента, класифікація та характеристика основних типів систем).

Тема 2. Показники надійності та безпеки КС.

Загальна характеристика показників надійності комп'ютерних систем (поняття і класифікація). Одиничні показники надійності (показники безвідмовності, загальний закон надійності, експонентний закон; показники ремонтопридатності; загальна характеристика показників довговічності і зберігання). Закони розподілу випадкових величин в надійності. Комплексні показники надійності (коефіцієнти готовності, оперативної готовності та технічного використання). Загальна характеристика показників відмовостійкості (класифікація, спеціальні показники). Загальна характеристика показників живучості та безпеки (класифікація, спеціальні показники живучості та безпеки).

Змістовний модуль 2. Оцінювання надійності КС.

Тема 3. Оцінювання надійності невідновлюваних КС.

Класифікація методів забезпечення надійності (загальна характеристика методів забезпечення надійності при розробці, виробництві і експлуатації; особливості забезпечення надійності апаратних і програмних засобів). Оцінювання надійності нерезервованих невідновлювальних систем (структурна схема надійності, урахування режимів роботи і умов експлуатації, послідовність розрахунку безвідмовності). Оцінювання надійності невідновлювальних резервованих систем. Методи резервування (основні поняття теорії резервування, класифікація методів резервування; паралельне резервування, мажоритарну резервування, резервування заміщенням). Оцінювання надійності систем з послідовно-паралельним з'єднанням елементів. Надійність мажоритарних систем з одно- і багатоярусної структурою. Особливості оцінювання адаптивних систем. Надійність систем при резервуванні заміщенням (облік режимів роботи резерву; ковзне резервування; порівняльний аналіз безвідмовності резервованих систем).

Тема 4. Оцінювання надійності відновлюваних КС.

Оцінювання надійності відновлюваних нерезервованих систем (основні співвідношення для розрахунку безвідмовності, ремонтопридатності і готовності). Оцінювання надійності відновлюваних резервованих систем (особливості відновлюваних резервованих систем, поняття про марковські випадкові процесі в теорії надійності; методика оцінки надійності (аналіз станів, граф переходів, рівняння Колмогорова-Чепмена в диференціальному і алгебраїчному вигляді і особливості їх аналізу, розрахунок показників

готовності і оперативної готовності). Використання інструментальних засобів для оцінювання.

Модуль 2. Методи забезпечення надійності та відмовостійкості КС

Змістовний модуль 3. Методи діагностування та оцінювання програмних засобів КС.

Тема 1. Методи діагностування апаратних і програмних засобів КС.

Основні поняття технічної діагностики (об'єкти, процеси, засоби і системи контролю і діагностування; властивості - достовірність контролю і достовірність функціонування, контролепридатність; логічна модель і помилки контролю і діагностування). Структурна організація систем контролю і діагностування (структурні схеми робочого, тестового і комбінованого контролю і діагностування; основні елементи структур - перетворювачі вхідних впливів і вихідних реакцій, формувач очікуваних реакцій, блок аналізу, генератор тестових впливів). Показники ефективності систем контролю і діагностування (показники достовірності контролю і діагностування, повнота контролю, глибина діагностування; оперативність контролю і діагностування; складність і надійність засобів контролю і діагностування). Класифікація методів контролю і діагностування (ознаки класифікації, загальна характеристика методів робочого і тестового контролю). Методи робочого контролю і діагностування (контроль дублюванням, мажоритарний контроль, контроль за модулем, програмно-логічні методи контролю, оцінка характеристик). Методи тестового контролю і діагностування (метод таблиць несправностей, метод активізації шляхів, методики отримання тестів перевірки працездатності і пошуку дефектів, псевдовипадкове тестування, сигнатурний аналіз, вбудовані засоби тестування НВІС, принципи апаратно-програмної реалізації систем тестового діагностування).

Тема 2. Методи оцінювання і забезпечення надійності програмних засобів.

Особливості оцінювання надійності програмних засобів КС (поняття надійності програмних засобів, класифікація та аналіз дефектів, показники надійності програмних засобів). Моделі якості. Огляд та вимоги стандартів IEC25010, IEC25010 та інш. Загальна характеристика моделей надійності програмних засобів (класифікація, аналіз основних моделей - метрик Холстеда, моделі Джелінскі-Моранді, Шумана та ін.). Вибір і верифікація моделей надійності (матриця припущень, процедури вибору і комплексування моделей). Застосування методик і інструментальних засобів. Огляд і аналіз методів забезпечення надійності програмних компонентів.

Змістовний модуль 4. Методи оцінювання та забезпечення та відмовостійкості КС.

Тема 3. Методи оцінювання безпеки КС.

Особливості оцінювання функціональної безпеки КС. Огляд та вимоги стандартів IEC61508, IEC26262, IEC15408 та інш. Класифікація і огляд методів оцінювання. Аналіз сутності та приклади застосування методів ХМЕСА, ХТА,

XIT, XBD. Особливості оцінювання функціональної безпеки КС з використанням марковських випадкових процесів. Урахування фактору кібербезпеки.

Тема 4. Методи забезпечення відмостійкості КС.

Загальна послідовність та зміст етапів забезпечення надійності та функціональної безпеки при створенні та використанні КС. Поняття про оптимальне резервування та обмеження при проектуванні надійних і відмовостійких і відмовобезпечних КС. Принципи одиничної відмови, незалежності та диверсності та їх впровадження. Методи і технології багатоверсійного проектування. Перспективні технології забезпечення надійності та функціональної безпеки КС. Підведення підсумків лекційної частини дисципліни.

Модульний контроль.

4. Структура навчальної дисципліни

Назви змістовних модулів і тем	Кількість годин				
	Усього	У тому числі			
		л	п	лаб.	с. р.
1	2	3	4	5	6
Модуль 1					
Змістовний модуль 1. Основні поняття та показники надійності та відмовостійкості КС.					
Тема 1. Загальна характеристика. Базові поняття теорії надій-ності та безпеки КС.	4	2			2
Тема 2. Показники надійності та безпеки КС. Модульний контроль	10	4			6
Разом за змістовним модулем 1	**14**	**6**			**8**
Змістовний модуль 2. Оцінювання надійності КС.					
Тема 3. Оцінювання надійності невідновлюваних КС.	26	8		8	10
Тема 4. Оцінювання надійності відновлюваних КС. Модульний контроль	20	2		4	14
Разом за змістовним модулем 2	**46**	**10**		**12**	**24**

Усього годин у модулі 1	**60**	**16**		**12**	**32**
Модуль 2					
Змістовний модуль 3. Методи діагностування та оцінювання програмних засобів КС.					
Тема 1. Методи діагностування апаратних і програмних засобів ІУС.	15	4		4	7
Тема 2. Методи оцінювання і забезпечення надійності програмних засобів. Модульний контроль	16	4		4	8
Разом за змістовним модулем 3	**31**	**8**		**8**	**15**
Змістовний модуль 4. Методи оцінювання та забезпечення та відмовобезпеки КС.					
Тема 3. Методи оцінювання безпеки КС.	19	4		4	11
Тема 4. Методи забезпечення відмовостійкості КС. Модульний контроль	25	4	8		13
Разом за змістовним модулем 4	**44**	**8**	**8**	**4**	**24**
Усього годин у модулі 2	**75**	**16**	**8**	**12**	**39**
Усього годин по дисципліні	**135**	**32**	**8**	**24**	**71**

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
1	Сучасні методи та засоби забезпечення надійності та відмовостійкості комп'ютерних систем	8
	Разом	8

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	*Не передбачено*	
	Разом	

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Розрахунок і дослідження надійності (безвідмовності і зберігання) промислових комп'ютерів з урахуванням режимів роботи і умов експлуатації.	4
2	Дослідження методів резервування і розрахунок надійності невідновлювальних КС.	4
3	Дослідження надійності відновлюваних КС з використанням апарату Марковських процесів.	4
4	Розробка тестів для контролю і діагностування цифрових схем КС.	4
5	Дослідження моделей надійності програмних засобів	4
6	Розробка і дослідження методів оцінки безпеки компонентів КС.	4
	Разом	**24**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Показники надійності (довговічності і збереженості). Ризики критичних відмов та методи його визначення.	6
2	Принципи програмно-апаратної реалізації відновлювальних пристроїв для різних методів резервування комп’ютерних систем.	9
3	Інструментальні засоби оцінювання надійності та безпеки комп’ютерних систем.	10
4	Методи он-лайн контролю мікропроцесорних систем.	8
5	Моделі зростання надійності (SRGM) програмних засобів.	10
6	Оцінка надійності і безпеки з використанням різних типів дерев відмов і атак.	8
7	Розрахунок готовності та оптимальне резервування компонентів комп’ютерних систем.	6
8	Типові архітектури та технології	14

	проектування відмовостійких і відмовобезпечних комп'ютерних систем.	
	Разом	**71**

9. Індивідуальні завдання

Розрахунково-графічне завдання за індивідуальним варіантом. Тема «Розрахунок готовності та оптимальне резервування компонентів ІУС» (за темою 2, змістовного модулю 2, модулю 2, 8 годин самостійної роботи)

10. Методи навчання

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

11. Методи контролю

Проведення поточного контролю, тестування знань, письмового модульного контролю, підсумковий контроль у вигляді екзамену.

12. Критерії оцінювання та розподіл балів, які отримують студенти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Підготовка до семінарського заняття (визначення теми, підбір та огляд літератури, формування плану звіту та презентації)	0...5	1	0…5
Змістовний модуль 2			
Виконання і захист лабораторних робіт	0…5	3	0…15
Модульний контроль	0…25	1	0…25
Змістовний модуль 3			
Виконання і захист лабораторних робіт	0...5	2	0…10
Змістовний модуль 4			
Виконання і захист розрахунково-графічного завдання	0...10	1	0…10
Виступ з доповіддю та захист звіту на семінарському занятті (підготовка презентації, звіту, доповіді)	0...10	1	0...10
Модульний контроль	0…25	1	0…25
Усього за семестр			**0…100**

Семестровий контроль у вигляді іспиту проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до іспиту. Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Білет для іспиту складається із двох теоретичних та одного практичного запитання, максимальна кількість балів за кожне теоретичне запитання, складає 34 балів, а за практичне – 32 балів.

Критерії оцінювання роботи студента протягом семестру

Задовільно (60 – 74). Показати мінімум знань та умінь. Показати позитивні результати по лабораторним роботам 1 – 5, розрахунково-графічному завданню та семінару.

Знати основні поняття і показники надійності та безпеки комп'ютерних систем; методи оцінювання надійності апаратних і програмних компонентів і комп'ютерних систем в цілому; методи забезпечення надійності комп'ютерних систем на різних етапах життєвого циклу.

Вміти аналізувати вимоги до надійності, виходячи з вимог технічних завдань на розроблення системи; розраховувати показники надійності, базуючись на електричних схемах і програмному забезпеченні систем з використанням відповідних методів оцінювання; вибирати елементну базу, методи і об'єм резервування відповідно до вимог.

Добре (75 – 89). Твердо знати мінімум. Показати позитивні результати по лабораторним роботам 1 – 5 (не нижче 3), отримати бали по розрахунково-графічному завданню (не нижче 5) та семінару (не нижче 5).

Знати основні поняття і показники надійності, відмовостійкості, живучості та безпеки комп'ютерних систем; методи оцінювання надійності апаратних і програмних компонентів і комп'ютерних систем в цілому; методи забезпечення надійності комп'ютерних систем на різних етапах життєвого циклу.

Вміти аналізувати вимоги до надійності, виходячи з вимог технічних завдань на розроблення системи; розраховувати показники надійності і функціональної безпеки системи, базуючись на електричних схемах і програмному забезпеченні систем з використанням відповідних методів оцінювання; вибирати елементну базу, методи і об'єм резервування відповідно до вимог.

Відмінно (90 – 100). Здати всі лабораторні роботи з оцінкою «добре» або «відмінно». Виконати у повному обсязі розрахунково-графічне завдання або його ускладнений варіант. Підготувати аналітичний звіт, презентацію, виступити на семінарі і захистити звіт.

Знати основні поняття і показники надійності, відмовостійкості, живучості та безпеки комп'ютерних систем; методи і засоби оцінювання надійності та безпеки апаратних і програмних компонентів і комп'ютерних систем в цілому; методи і засоби забезпечення надійності та безпеки комп'ютерних систем на різних етапах життєвого циклу; перспективні напрями розвитку та впровадження засобів забезпечення відмовостійкості та безпеки.

Вміти аналізувати вимоги до надійності, виходячи з вимог стандартів та технічних завдань на розроблення системи; розраховувати показники надійності і функціональної безпеки системи, базуючись на електричних схемах і програмному забезпеченні систем з використанням відповідних методів і засобів оцінювання; приймати рішення щодо забезпечення вимог до надійності шляхом прийняття відповідних проектних рішень, вибору елементної бази, видів резервування, методів контролю і діагностування.

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. Харченко В. С. Конспект лекцій (Харченко В. С. (ред). Надійність цифрових систем. Підручник. МОН України, 2006, 342 с.)
2. Лисенко І. В., Тарасюк О. М., Харченко В. С., Надійність і відмовостійкість комп'ютерних систем. Методичний посібник до лабораторних робіт, ХАІ, 2012, 98 с.
3. Харченко В. С. Методичні вказівки до підготовки до семінару.
4. Харченко В. С. Методичні вказівки до виконання розрахунково-графічної роботи.

14. Рекомендована література

Базова

1. Основи діагностики цифрових систем. Підручник/ За ред. Харченка В.С., Ілюшка В.М. - Харків: Міністерство освіти та науки, 2007. 360 с.
2. Основи надійності цифрових систем. Підручник/ За ред. Харченка В.С., Жихарева В.Я. - Харків: Міністерство освіти та науки, 2006. 342 с.
3. Харченко В.С., Скляр В.В., Тарасюк О.М. Методы моделирования и оценки качества и надежности программного обеспечения. Учебное пособие. – Харьков: ХАИ, 2008. 221 с.
4. Харченко В.С., Тарасенко В.В., Ушаков А.А. Отказоустойчивые встроенные цифровые системы на ПЛИС.- Учебное пособие. – Харьков: ХАИ, 2012. 189 с.

5. Отказобезопасные информационно-управляющие системы на программируемой логике/ Под ред. Харченко В.С., Скляра В.В. НАКУ «ХАИ», НПП «Радий», 2013. 291 с.

6. Харченко В.С., Лысенко И.В., Тарасюк О.М. Надежность и отказоустойчивость компьютерных систем. Руководство к лабораторным работам. – Харьков: ХАИ, 2013. 98 с.

Допоміжна

1. Козлов Б.А., Ушаков И.А. Справочник по расчету надежности аппаратуры радиоэлектроники и автоматики. — М.: Сов. радио, 1975. 349с.

2. Харченко В.С., Скляр В.В., Конорев Б,М. и др. Оценка и обеспечение качества программных средств космических систем. Национальное космическое агентство Украины, НАКУ «ХАИ», Сертцентр АСУ, 2013. 294 с.

3. Основи цифрових систем. Підручник/ За ред. Благодарного М.П., Харченка В.С. - Харків: Міністерство освіти та науки, 2004. 351 с.

4. Федоров Ю.Н. Справочник инженера по АСУ ТП. – М.: Инфра-инженерия, 2012.

5. Методи системного аналізу у комп'ютерній інженерії та радіоелектроніці: підручник / За ред. С.Ю. Даншиної, В.С. Харченка.– Х.: Нац. аерокосм. ун-т «Харьк. авіац. ін-т», 2013. 312 с.

6 . Издания ХАИ по проектам MASTAC (2009-2010), SAFEGUARD (2011-2013), GREENCO (2014-2015), SEREIN (2015-2018), ALIOT (2019).

15. Інформаційні ресурси

1. Бабчук С.М. Надійність комп'ютерних систем і мереж, 2017 [Электрон. ресурс]. – http://194.44.112.13/chytalna/5417/index.html#p=1.

2. Вишнівський В.В. Основи надійності та діагностики телекомунікаційних систем, 2016 [Электрон. ресурс]. – Режим доступа: http://www.dut.edu.ua/uploads/l_1092_31009342.pdf

3. The First 50 Years of Software Reliability Engineering: A History of SRE withFirst Person AccountsJames J. Cusick, PMP, New York, 2017 [Электрон. ресурс]. – Режим доступа: https://arxiv.org/ftp/arxiv/papers/1902/1902.06140.pdf/

4. Operating System Reliability from the Quality of Experience Viewpoint: An Exploratory Study [Электрон. ресурс]. – Режим доступа: https://www.researchgate.net/publication/236332149_Operating_System_Reliability_from_the_Quality_of_Experience_Viewpoint_An_Exploratory_Study

5. Advances in System Reliability Engineering [Электрон. ресурс]. – Режим доступа: https://www.elsevier.com/books/advances-in-system-reliability-engineering/ram/978-0-12-815906-4.