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

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

ЗАТВЕРДЖУЮ

Гарант ОНП
«Комп'ютерна інженерія»
_____ Є.В. Бабешко
(підпис) (ініціали та прізвище)

«31» 08 2020 р.

СИЛАБУС ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Формальні методи розробки та верифікації програмних систем
(назва навчальної дисципліни)

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

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

Освітньо-наукова програма: «Комп'ютерна інженерія»
(назва освітньої програми)

Форма навчання: денна

Рівень вищої освіти: третій (освітньо-науковий)

Харків 2020 рік

Силабус Формальні методи розробки та верифікації програмних систем
(назва дисципліни)

для аспірантів за спеціальністю: 123 «Комп'ютерна інженерія»
(код та найменування спеціальності)

Освітньо-науковою програмою «Комп'ютерна інженерія»
(найменування програми)

«26» 08 2020 р., – 10 с.

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

(підпис)

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

Протокол № 1 від «27» 08 2020 р.

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

1. Опис навчальної дисципліни

Галузь знань – 12 «Інформаційні технології»
Спеціальність – 123 «Комп'ютерна інженерія»
Освітня програма – «Комп'ютерна інженерія»
Рівень вищої освіти – третій (освітньо-науковий)
Форма навчання – денна
Семестр, в якому викладається дисципліна – 4
Дисципліна вибіркова
Загальна кількість годин за навчальним планом – 165 годин/5,5 кредитів ЄКТС.
Види занять – лекції, практичні роботи
Вид контролю – іспит

2. Мета та завдання навчальної дисципліни

Мета: засвоїти знання з методів та інструментальних засобів розроблення і верифікації програмних систем і програмно-технічних комплексів з використанням формальних і напівформальних методів в наукових дослідженнях.

Завдання: підготувати фахівців, здатних застосовувати і удосконалювати кейс-орієнтовані методи і засоби розроблення і верифікації програмних систем і програмно-технічних комплексів з використанням формальних и напівформальних процедур

Компетентності, які набуваються:
- 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 комп'ютерної інженерії.

Очікувані 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 комп'ютерній інженерії 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.

Пререквізити. Матеріал дисципліни базується на знаннях, отриманих під час вивчення дисциплін із циклу обов'язкових компонент, а саме «Обробка та аналіз результатів наукових досліджень з використанням ІТ», «Управління науковими проектами».

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

3. Програма навчальної дисципліни

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 МЕК 61508.

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 стандартом МОС/МЕК 15408.

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.

Обгрунтування 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. Індивідуальні завдання

Не передбачено

5. Методи навчання

Проведення аудиторних лекцій, практичних робіт, консультацій, а також самостійна робота аспірантів з використанням відповідних матеріалів.

6. Методи контролю

При вивченні дисципліни «Формальні методи розробки та верифікації програмних систем» використовуються такі види контролю:

- поточний,
- підсумковий.

Поточний контроль – контроль рівня знань та умінь у процесі навчання, що проводиться на лекціях та практичних заняттях. Його види та форми:

- опитування на засвоєння попередньої лекції (на початку чергової лекції);
- опитування під час лекції на розуміння її суті;
- контроль за засвоєнням матеріалу лекції;
- співбесіда;
- електронне тестування;
- модульний контроль.

Підсумковий контроль – це контроль, що здійснюється в кінці вивчення дисципліни у вигляді іспиту.

7. Критерії оцінювання та розподіл балів, які отримують аспіранти

7.1. 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	5	0…5
Виконання практичних робіт	0…5	2	0...10
Модульний контроль	0…10	1	0…10
Змістовний модуль 2			
Робота на лекціях	0…1	5	0…5
Виконання практичних 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).

7.2. Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки

1. Знати існуючий формальний та неформальний апарат оцінювання безпеки комп'ютеризованих систем;
2. Знати основні поняття інформаційно-комунікаційних систем, життєвих циклів;
3. Знати основні етапи розробки та верифікації інформаційно-керуючих систем;

4. Знати різновиди безпеки та взаємозв'язок між ними;
5. Знати основні міжнародними стандарти та керівні принципи в сфері функціональної, інформаційної та кібербезпеки;
6. Знати класифікацію підходів для аналізу та обґрунтування безпеки;
7. Знати принципи рецензування і написання наукових статей.

Необхідний обсяг умінь для одержання позитивної оцінки

1. Уміти використати найсучасніші полу-формальні методи аналізу функційної безпеки та інформаційної безпеки комп'ютеризованих систем при виконанні наукових досліджень;
2. Уміти здійснювати рецензування статей і писати наукові статті, перевіряти їх на плагіат;
3. Уміти користуватись сучасними інформаційними технологіями для проведення наукових досліджень.

7.3 Критерії оцінювання роботи аспіранта протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Виконати рецензування двох статей: україномовної та англомовної. Знати базові поняття, що стосуються інформаційних технологій і вміти використовувати сучасні інформаційні технології.

Добре (75-89). Твердо знати теоретичний мінімум, відвідати і виконати не менше 90% практичних занять. Отримати з редакції наукового журналу, зазначеного у переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук 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. Уміти 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 і кандидата наук, 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

8. Методичне забезпечення

1. Ілляшенко, О.О., Брежнєв, Е.В., Орєхова, А.О.: Основи IT-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)

9. 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 зфtand 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)

Допоміжна:

1. Williams, J. R., George F. J.: A framework for reasoning about assurance, document number ATR 97043. In: Arca Systems, Inc. 23 April 1998
2. 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
3. Kelly, T.P.: Arguing Safety – a systematic approach to safety case management. In: Ph.D. Thesis, Department of Computer Science, University of York, UK (1999)
4. Wilson, S., Kirkham, P. Safety: Argument manager (SAM) user manual. In: University of York, York. December 1995
5. Bishop, P.G., Bloomfield, R.E.: A methodology for safety case development. In: Redmill, F., Anderson, T. (eds.) Industrial Perspectives of Safety-critical Systems: Proceedings of the Sixth Safety-Critical Systems Symposium. Birmingham, pp 194–203. Springer, London (1998)
6. Kelly, T.P., Weaver, R.A.: The goal structuring notation - A safety argument notation. In: Proceedings of the Dependable Systems and Networks 2004, Workshop on Assurance Cases, July 2004
7. ASCAD – Adelard safety case development manual. In: Adelard. (2010)
8. Draft GSN Standard, version 1.0. In: York University (2010)
9. Gorski, J.: Trust Case – a case for trustworthiness of IT infrastructures. In: Kowalik, J.S. et al (eds.), Cyberspace Security and Defense: Research Issues. pp.125-141. Springer. Printed in the Netherlands. (2005)
10. Cyra, Ł.: A method of trust case templates to support standards conformity achievement and assessment. (2008)
11. 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)
12. Górski, J.: Trust-IT – A framework for trust cases, workshop on assurance cases for security - The Metrics Challenge. In: The 37th Annual IEEE/IFIP International Conf. on Dependable Systems and Networks, Edinburgh, UK. 25 – 28 June 2007
13. National Defense Industrial Association (NDIA) system assurance committee. Engineering for System Assurance. In: Arlington, VA: NDIA. (2008).

14. 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). Accessed 28 Sep 2018

15. Adelard safety case development manual, http://www.adelard.com/resources/ascad/ascad_download.html (2015) Accessed 29 Sep 2018

16. Toulmin, S.E.: The uses of argument. In: Cambridge University Press, Cambridge, England (1958)

17. The Adelard Safety Case Editor – ASCE. In: Adelard. http://www.adelard.co.uk/software/asce/index.html (2010). Accessed 27 Sep 2018

18. Assurance and Safety Case Environment (ASCE) help manual. In: Adelard, Version 4.1. http://www.adelard.com/asce/v4.1/download.html (2010). Accessed 27 Sep 2018

19. Stockham, R.: Emphasis on safety. In: Engineering & Technology Magazine. Vol. 4, Issue 2, pp. 47 – 49 (2009). Accessed 30 Sep 2018

20. 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)

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

22. COBRA - security risk analysis & assessment. http://www.riskworld.net/ (2018). Accessed 28 Sep 2018

23. Condor - A system for developing and managing information security policies. Digital Security http://www.dsec.ru/products/kondor/ (2018). Accessed 28 Sep 2018

24. SESAMO. Security and safety modelling. http://sesamo-project.eu. (2018). Accessed 12 Nov 2018

Стандарти:

1. IEC 61508:2010: Functional safety of electrical/electronic/ programmable electronic safety-related systems Part 1: General requirements International Organization for Standardization (2010)

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 (2012)

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 (2012)

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 (2012)

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 (2009)

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

10. 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