ДЕРЖАВНИЙ ТОГРОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015
Кафедра інженерії програмного забезпечення та кібербезпеки

ЗАТВЕРДЖЕНО
вченою радою
(пост. п.__ від «__» __03__ 2024 р.)
Ректор
_____ Анатолій МАЗАРАКІ

МОНІТОРИНГ ТА ТЕСТУВАННЯ СИСТЕМ КІБЕРБЕЗПЕКИ /
MONITORING AND TESTING OF CYBERSECURITY SYSTEMS

ПРОГРАМА /
COURSE SUMMARY

Київ 2024

Автори: Ю.Є. ХОХЛАЧОВА, кандидат технічних наук, професор . кафедри безпеки інформаційних технологій Національного авіаційного університету ,
Д.Д. ЧЕРНИШОВА, асистент кафедри інженерії програмного забезпечення та кібербезпеки

Програму розглянуто і затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки «22» січня 2024р., протокол № 20.

Рецензенти: Н.О. КОТЕНКО, канд. пед. наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки,
В.П. ЗВЄРЄВ, кандидат технічних наук, заступник керівника служби з питань інформаційної безпеки та кібербезпеки – керівник управління інформаційної безпеки Апарату Ради Національної безпеки і оборони України

МОНІТОРИНГ ТА ТЕСТУВАННЯ СИСТЕМ КІБЕРБЕЗПЕКИ / MONITORING AND TESTING OF CYBERSECURITY SYSTEMS

ПРОГРАМА /

COURSE SUMMARY

ВСТУП

Дисципліна «Моніторинг та тестування систем кібербезпеки» є обов'язковою компонентою навчального плану підготовки студентів денної та заочної форм навчання другого (магістерського) рівня вищої освіти галузі знань 12 «Інформаційні технології», спеціальності 125 «Кібербезпека та захист інформації», освітньої програми «Безпека систем електронних комунікацій в економіці».

Програму підготовлено відповідно до Стандарту вищої освіти України із зазначеної спеціальності та відповідної освітньо-професійної програми підготовки магістрів ДТЕУ.

Програма складається з таких частин:

1. Мета, завдання та предмет дисципліни.
2. Передумови вивчення дисципліни як вибіркової компоненти освітньої програми.
3. Результати вивчення дисципліни.
4. Зміст дисципліни.
5. Список рекомендованих джерел.

1. МЕТА, ЗАВДАННЯ ТА ПРЕДМЕТ ДИСЦИПЛІНИ

Метою викладання навчальної дисципліни «Моніторинг та тестування систем кібербезпеки» є формування системи теоретичних знань та практичних умінь про сучасні наукові концепції, поняття, принципи і методики аналізу та опрацювання консолідованих інформаційних ресурсів та інженерії знань, що є практичною основою для фахівця в галузі кібербезпеки.

Завданням дисципліни є: оволодіння технологіями моделювання інформаційних систем в умовах невизначеності, моделювання кіберресурсів, оволодіння механізмами кіберресурів із забезпеченням безпеки.

Предметом вивчення дисципліни є технології моделювання інформаційних систем в умовах невизначеності та моделювання кіберресурсів.

2. ПЕРЕДУМОВИ ВИВЧЕННЯ ДИСЦИПЛІНИ ЯК ВИБІРКОВОЇ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ

знання:

- інформаційних технологій;
- безпека інформаційних систем та мереж;
- іноземної мови за професійним спрямуванням;
- основ кібербезпеки.

вміння: вільно працювати:

- з офісними додатками Microsoft;
- з хмарними сервісами Office 365;
- з пошуковою системою Google.

3. РЕЗУЛЬТАТИ ВИВЧЕННЯ ДИСЦИПЛІНИ

Дисципліна «Моніторинг та тестування систем кібербезпеки» як обов'язкова компонента освітньої програми, забезпечує оволодіння студентами загальними та фаховими компетентностями і досягнення ними програмних результатів навчання за відповідною освітньо-професійною програмою:

«Безпека систем електронних комунікацій в економіці (ОС «магістр»)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Загальні компетентності за освітньою програмою		
КЗ-1.	Здатність застосовувати знання у практичних ситуаціях.	1-12
КЗ-3.	Здатність до абстрактного мислення, аналізу та синтезу.	1-12
КЗ-4.	Здатність оцінювати та забезпечувати якість виконуваних робіт.	1-12
Спеціальні (фахові, предметні) компетентності за освітньою програмою		
КФ1.	Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.	1-12
КФ2.	Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.	1-12
КФ3.	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.	1-12
КФ9.	Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.	1-12
КФ11.	*Здатність аналізувати електронні комунікаційні мережі та протистояти діям, що становлять загрозу доступності, цілісності чи конфіденційності таких*	1-12

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
	мереж і послуг, а також даних, що зберігаються, передаються чи обробляються, та пов'язаних із ними послуг, зокрема в економіці.	
КФ12.	*Здатність виконувати обов'язки внутрішнього консультанта і радника у своїй експертній області.*	1-12
КФ13.	*Здатність проводити дослідно-експериментальну роботу щодо процедури сканування вразливостей та їх розпізнавання в системах безпеки.*	1-12
Програмні результати навчання за освітньою програмою		
РН5	Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.	1-12
РН6	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	1-12
РН14	Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.	1-12
РН15	Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.	1-12
РН23	Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також	1-12

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
	обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	

4. ЗМІСТ ДИСЦИПЛІНИ

Тема 1. Предмет дисципліни, її цілі.

Основні види документів. Визначення режиму доступу до інформації згідно Закон України "Про інформацію". Законодавчі акти і нормативні документи щодо захисту інформації. Закон України „Про інформацію”. Закон України „Про науково-технічну інформацію”. Закон України „Про телекомунікації”. Закон України „Про Національний архівний фонд та архівні установи”. Закон України „Про державну таємницю”.

Список рекомендованих джерел:

Основний: 1, 4, 5
Додатковий: 1, 4
Інтернет-ресурси: 1, 2

Тема 2. Основні терміни та визначення.

Визначення термінів. Об'єкти захисту. Суб'єкти відносин. Право власності на інформацію в системі. Доступ до інформації. Відносини між суб'єктами в процесі обробки інформації в системі.

Список рекомендованих джерел:

Основний: 1, 2, 3, 4, 5
Додатковий: 1, 5
Інтернет-ресурси: 1, 2

Тема 3. Організація захисту інформації в системі.

Основні питання та організаційні особливості. Відповідальність за порушення законодавства у сфері захисту інформації в системі. Міжнародне співробітництво у сфері захисту інформації в системі.

Список рекомендованих джерел:

Основний: 1, 3, 4, 5
Додатковий: 1, 3, 5
Інтернет-ресурси: 1, 2

Тема 4. Поняття моніторингу.

Поняття моніторингу. Можливі цілі моніторингу. Різновиди моніторингу. Предмет спостережень. Поняття події.

Список рекомендованих джерел:

Основний: 1, 2
Додатковий: 1, 4, 5
Інтернет-ресурси: 1, 2

Тема. 5. Характеристики та види подій при моніторингу.

Статистичні і сукупні характеристики подій. Види подій, що реєструються при моніторингу. Види показників спостережуваних подій. Поняття та види порогів.

Список рекомендованих джерел:

Основний: 1, 2
Додатковий: 1, 2, 4
Інтернет-ресурси: 1, 2

Тема 6. Види моніторингу та основні питання.

Стратегічний моніторинг. Основні об'єкти стратегічного моніторингу. Оперативний моніторинг. Аналіз даних оперативного моніторингу. Моніторинг масової активності. Основні показники та цілі моніторингу масової активності. Моніторинг установ. Цілі моніторингу установ.

Список рекомендованих джерел:

Основний: 1, 3
Додатковий: 1, 2, 4, 5
Інтернет-ресурси: 1, 2

Тема 7. Сучасні методи та технології моніторингу.

Радіомоніторинг, його завдання та категорії вирішення завдань. Основні складові радіомоніторингу. Контент-моніторинг. Сучасні методи контент-моніторингу. Технологія TextMining. Моніторинг соціальних медіа. Моніторинг в Інтернеті. Класифікатор пошукових засобів в мережі Інтернет. Інформаційно-аналітичні системи в Інтернет. Небезпека Інтернету як джерела інформації для розвідки (моніторингу).

Список рекомендованих джерел:

Основний: 1, 2, 3
Додатковий: 1, 2, 4
Інтернет-ресурси: 1, 2

Тема 8. Прогнозування (передбачення). Загальні питання.

Процес прогнозування, його види та методи. Способи передбачення (прогнозування). Компоненти системи прогнозування. Методи неформальної прогнозування. Правила складання прогнозів. Задачі прогнозування в інформаційно-аналітичній роботі.

Список рекомендованих джерел:

Основний: 1, 2, 3, 4
Додатковий: 1, 3, 5
Інтернет-ресурси: 1, 2

Тема 9. Підходи та методи моніторингу.

Підхід до програмної реалізації агресивності програмних засобів. Концепція безпеки програмного засобу та її властивості. Підходи до відновлення алгоритмів. Методи визначення факта інформаційного вторгнення

Список рекомендованих джерел:

Основний: 1, 2, 3
Додатковий: 1, 2, 4
Інтернет-ресурси: 1, 2

Тема 10. Методи тестування криптографічних програмних систем.

Структурний метод (метод білого або скляного ящика). Поведінковий метод «чорного ящика». Метод регресивного тестування. Метод «сірого ящика». Метод дослідної експлуатації. Тестування ергономічності.

Список рекомендованих джерел:

Основний: 1, 3
Додатковий: 1, 4, 5
Інтернет-ресурси: 1, 2

Тема 11. Основні принципи процесу тестування.

Основні принципи тестування. Їх концепції та підходи. Рівні та принципи тестування програмного забезпечення. Планування тестування. Підготовка. Тестування. Аналіз результатів тестування.

Список рекомендованих джерел:

Основний: 1, 2, 3
Додатковий: 1, 2, 5
Інтернет-ресурси: 1, 2

Тема 12. Методика забезпечення якості програмного забезпечення

Основні поняття та визначення. Міжнародні стандарти. Методи визначення якості програмного забезпечення. Сучасні програмні засоби для визначення якості програмного забезпечення. Характеристики якості ПЗ. Моделі якості ПЗ. Рекомендації та метрики с забезпечення якості.

Список рекомендованих джерел:

Основний: 1, 2, 3, 4, 5
Додатковий: 1, 2, 3, 4, 5
Інтернет-ресурси: 1, 2

5. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

1. Хохлачова Ю.Є. Моніторинг та тестування систем кібербезпеки: лабораторний практикум / Ю.Є. Хохлачова, В.М. Кінзерявий, В.В. Погорелов та ін. К.: НАУ, 2022. 56 с.

2. Браіловський М.М., Зибін С.В., Пискун І.В., Хорошко В.О., Хохлачова Ю.Є. Технології захисту інформації. К.: ЦП «Компринт», 2021. 296 с.

3. Луцький М.Г., Хорошко В.О., Хохлачова Ю.Є., Козловський В.В., Баланюк Ю.В., Прав Ю.Г. Новітні технології захисту інформації: підручник. К.: НАУ, 2023. 312 с.

4. Пирцхалава Л.Г., Хорошко В.О., Хохлачова Ю.Є., Шелест М.Є. Інформаційно-аналітичне забезпечення безпеки. – Київ: ФЛП Ямчинський О.В. 2021. 470 с.

5. Безпека інформаційних систем: навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ: Держ. торг.-екон. ун-т, 2022. – 376 с.

Додатковий

1. Хорошко О.В. Захист систем електронних комунікацій: навч.посіб./ В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ: Київ. нац. торг.-екон. ун-т, 2019. – 164 с.

2. М.М. Браіловський, Н.С. Вишневська, В.Д. Козюра, Ю.В. Пепа, В.О. Хорошко, Ю.Є. Хохлачова. Комп'ютерні технології: навчальний посібник. К.: ФОП Ямчинський О.В., 2023. 200 с.

3. Баланюк Ю.В., Козловський В.В., Хорошко В.О., Хохлачова Ю.Є. Інформаційно-психологічні впливи у кіберпросторі: навчальний посібник. К.: ЦП «Компринт», 2020. 09 с.

4. М.М. Браіловський, В.Д. Козюра, В.В. Кузавков, Ю.В. Пепа, Ю.М. Ткач, В.О. Хорошко. Спеціалізовані програмні засоби наукових досліджень: навчальний посібник. К.: ФОП Ямчинський О.В., 2022. 204 с.

5. Браіловський М.М., Зибін С.В., Кобозєва А.А., Хорошко В.О., Хохлачова Ю.Є. Аналіз кіберзахищеності інформаційних систем Київ: ФОП Ямчинський О.В., 2021. 360 с.

Інтернет-ресурси

1. www.rada.gov.ua – офіційний сайт Верховної Ради України.
2. www.dstszi.gov.ua/dstszi - офіційний сайт ДСТЗІ.

**Курсивом зазначені джерела, що є в наявності в бібліотеці ДТЕУ*