КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-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
(прот. п. ___ від «___» ___ 2021 р.)
Ректор
_____ А.А. Мазаракі

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ / SECURITY OF INFORMATION SYSTEMS

ПРОГРАМА / COURSE SUMMARY

Київ 2021

Автори: В.А. ЛАХНО, доктор технічних наук, професор
кафедри інженерії програмного забезпечення та кібербезпеки
М.В. САШНЬОВА, кандидат технічних наук, доцент
кафедри інженерії програмного забезпечення та кібербезпеки
Ю.В. КОСТЮК, асистент кафедри інженерії програмного
забезпечення та кібербезпеки

Програму розглянуто і затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки «20» квітня 2021 р., протокол №8.

Рецензенти: С.Л. РЗАЄВА, кандидат технічних наук, доцент
О.О. РУДЕНКО, Front-end Team Lead at Astound Commerce
О.А. ХАРЧЕНКО, декан факультету інформаційних технологій, кандидат технічних наук, доцент
С.М. МИРОНЕЦЬ, завідувач кафедри психології, доктор психологічних наук, доцент
В.А. ОСИКА, декан факультету торгівлі та маркетингу, доктор технічних наук, професор

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ /
SECURITY OF INFORMATION SYSTEMS

ПРОГРАМА /
COURSE SUMMARY

ВСТУП

Програма дисципліни «Безпека інформаційних систем» призначена для здобувачів другого рівня вищої освіти «Магістр» галузі знань 12 «Інформаційні технології», спеціальності 124 «Системний аналіз», спеціалізації «Інформаційні технології та бізнес-аналітика (Data Science)».

Програму підготовлено відповідно до вимог Стандартів вищої освіти України зі спеціальності 124 «Системний аналіз» та освітньо-професійної програми КНТЕУ «Інформаційні технології та бізнес-аналітика (Data Science)» другого (магістерського) рівня вищої освіти.

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 дисципліни є формування теоретичних знань та практичних навичок, необхідних для ефективного використання інформаційних технологій в інформаційних системах і мережах а також запобігання розголошенню, витоку і неправомірному оволодінню інформацією, протиправним діям щодо знищення, модифікації, копіювання і блокування інформації.

Предметом дисципліни є вивчення основних положень та принципів забезпечення інформаційної безпеки автоматизованих інформаційних систем і мереж та практичне опанування сучасних методів їх захисту.

Задачі вивчення дисципліни полягають у тому, щоб ознайомити студентів із законодавчим, організаційним, інженерно-технічним і програмними рівнями безпеки інформаційних систем, засобами і методами управління контролем доступу в комп’ютерних системах, методами ідентифікації і аутентифікації користувачів і ресурсів інформаційних систем, особливостями захисту інформації в локальних і корпоративних мережах, навчити їх реалізовувати практично правила політики безпеки.

2. ПЕРЕДУМОВИ ВИВЧЕННЯ ДИСЦИПЛІНИ ЯК ВИБІРКОВОЇ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ

знання:

- організація комп'ютерних мереж;
- безпека операційних систем;
- захист систем електронних комунікацій;
- архітектури комп'ютера;
- основ кібербезпеки;
- об'єктно-орієнтованого програмування;
- комп'ютерної дискретної математики;
- економічної інформатики (стандартне програмне забезпечення персональних комп'ютерів);
- технологія Java;
- правове забезпечення інформаційної безпеки держави;
- іноземної мови за професійним спрямуванням;

вміння: вільно працювати:

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

3. РЕЗУЛЬТАТИ ВИВЧЕННЯ ДИСЦИПЛІНИ

Дисципліна «Безпека інформаційних систем», як вибіркова компонента освітньої програми «Інформаційні технології та бізнес-аналітика (Data Science)», забезпечує оволодіння студентами загальними та фаховими компетентностями і досягнення ними програмних результатів навчання за відповідною освітньо-професійною програмою:

«Інформаційні технології та бізнес-аналітика (Data Science)»(ОС магістр 2021 рік)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Загальні компетентності		
ЗК3.	Здатність до пошуку, оброблення та аналізу інформації з різних джерел	1, 2, 3, 6
Спеціальні (фахові, предметні) компетентності		
СК2.	Здатність проєктувати архітектуру	4, 5, 6

	інформаційних систем.	
СК3.	Здатність розробляти системи підтримки прийняття рішень та рекомендаційні системи.	2, 5
СК7.	Здатність управляти робочими процесами у сфері інформаційних технологій, які є складними, непередбачуваними та потребують нових стратегічних підходів.	3, 4
СК13.	*Здатність розробляти і впроваджувати моделі задач інтелектуального аналізу даних засобами комп'ютерного моделювання.*	1,5,6
Програмні результати навчання		
РН 1.	Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері системного аналізу та інформаційних технологій і є основою для оригінального мислення та проведення досліджень.	1, 2, 4
РН 4.	Розробляти та застосовувати методи, алгоритми та інструменти прогнозування розвитку складних систем і процесів різної природи.	4, 5, 6
РН 5.	Використовувати міри оцінювання ризиків та застосовувати їх при аналізі багатофакторних ризиків в складних системах.	2, 3, 5
РН 8.	Здійснювати ідентифікацію та оцінювання параметрів математичних моделей об'єктів керування.	5, 6

4. ЗМІСТ ДИСЦИПЛІНИ

Тема 1. Основні положення теорії безпеки інформаційно-телекомунікаційних систем

Актуальність безпеки ІТС. Основні терміни та визначення безпеки ІТС. Моделі безпеки ІТС. Кіберпростір і кібербезпека. Ключові питання кібербезпеки. Кіберзброя, кібертероризм і кібервійни. Загрози безпеки функціонування ІТС. Класифікація загроз безпеки. Загрози доступності. Загрози цілісності. Загрози конфіденційності. Основні навмисні загрози. Несанкціонований доступ до системи або мережі. Сучасні мережеві загрози: інтернет-шахрайство. Сучасні мережеві загрози: крадіжка особистості. Загрози приватності і анонімності при роботі в відкритих мережах. Визначення та класифікація атак на ІТС. Мережеві атаки. Застосування бот-мереж. Порушники безпеки ІТС. Класифікація порушників. Сучасні технології захисту інформаційних ресурсів. Основні методи забезпечення безпеки інформаційних систем і мереж.

Список рекомендованих джерел:

Основний: 1,2,3,4
Додатковий: 6,9,12-14
Internet-ресурси: 15-17,19,20

Тема 2. Шкідливе програмне забезпечення і захист від руйнуючих програмних дій

Види можливих порушень в роботі інформаційної системи в професійній діяльності психолога. Поняття та класифікація шкідливого програмного забезпечення. Поняття і класифікація комп'ютерних вірусів. Коротка характеристика вірусів. Мережні хробаки. «Троянські програми». Спеціальні шкідливі програми. Соціальна інженерія. Методи виявлення шкідливих програм. Типи і характеристики антивірусних програм. Технологія Whitelisting.

Список рекомендованих джерел:

Основний: 1,2,3,4
Додатковий: 6,9,12-14
Internet-ресурси: 15-17,19,20

Тема 3. Правове забезпечення кібербезпеки

Структура законодавства по захисту інформації щодо окремих методик в пакетах прикладних програм та щодо інтерпретації комп'ютерної психодіагностики. Основні нормативні керівні документи, що стосуються державної таємниці. Нормативно-довідкові документи. Призначення і завдання у сфері забезпечення інформаційної безпеки на рівні держави.

Законодавство України по забезпеченню кібербезпеки. Структура законодавства по кібербезпеці. Нормативні документи системи технічного захисту інформації. Стандарти комп'ютерної безпеки. Критерії оцінювання захищеності інформаційної системи. Стандарт TCSEC. Класи безпеки комп'ютерних систем. Міжнародний стандарт побудови ефективної системи безпеки (серія ISO 27000). Державний стандарт України із захисту інформації. Поняття кіберзлочинності. Класифікація кіберзлочинів.

Список рекомендованих джерел:

Основний: 1,2,3,4

Додатковий: 6-9,10,11

Internet-ресурси: 19,20

Тема 4. Адміністративне та організаційне забезпечення інформаційно-телекомунікаційних систем

Організаційний захист. Політика безпеки в психологічній та медичній практиці. Структура політики безпеки організації. Програма безпеки. Процедури реалізації політики безпеки. Управління ризиками. Стандарти інформаційної безпеки. Критерії оцінювання захищеності інформаційної системи. «Критерії оцінки довірених комп'ютерних систем» («Помаранчева книга»). Аналіз засобів порушення інформаційної безпеки в психологічній та медичній практиці.

Список рекомендованих джерел:

Основний: 1,2,3,4

Додатковий: 7-14

Internet-ресурси: 16,18,20

Тема 5. Інженерно–технічне забезпечення інформаційно-телекомунікаційних систем

Інженерно-технічний рівень інформаційної безпеки в психологічній та медичній практиці. Технічні засоби для несанкціонованого доступу до інформації. Засоби протидії несанкціонованому доступу до інформації. Канали витоку інформації. Захист інформації від витоку по технічним каналам. Принципи захисту від промислового шпигунства. Засоби протидії несанкціонованому доступу до інформації.

Список рекомендованих джерел:

Основний: 1,2,3,4,5

Додатковий: 7,10,11,14

Internet-ресурси: 18,19,20

Тема 6. Апаратні та програмні засоби захисту

Загальна характеристика програмних засобів безпеки ІТС. Ідентифікація, автентифікація та авторизація суб'єктів ІТС. Види автентифікації суб'єктів ІТС. Парольна автентифікація. Апаратна автентифікація. Автентифікація за допомогою біометричних даних. Автентифікація на основі цифрових сертифікатів. Централізовані системи автентифікації. Концепція єдиного логічного входу. Управління доступом. Дискреційна модель розмежування доступу. Мандатна модель розмежування доступу. Рольова модель розмежування доступу. Реєстрація подій і аудит. Управління доступом. Реєстрація подій і аудит. Функціональне призначення та реалізація парольного захисту. Паролі в ОС Windows. Мережева аутентифікація в Windows. Апаратні засоби аутентифікації в психології.

Список рекомендованих джерел:

Основний: 1,2,3,4,5
Додатковий: 7,10,11,14
Internet-ресурси: 18,19,20

Тема 7. Основи криптографічного захисту інформації

Основні терміни та поняття криптографії. Історія та законодавча база криптографії. Перші методи шифрування перестановки та заміни. Одноалфавітні системи шифрування Віженера, Плейфейра та інші. Багатоалфавітні системи шифрування: Бьюфорта, Віженера та інші. Сучасні криптосистеми та їх особливості. Електронний цифровий підпис. Управління ключами та сертифікація ключів. Стеганографічні методи захисту інформації.

Список рекомендованих джерел:

Основний: 2,3,4,5
Додатковий: 9,12,13
Internet-ресурси: 15-18,20

Тема 8. Технології безпеки на основі фільтрації та моніторингу мережевого трафіку

Фільтрація трафіку. Фільтрація Web-змісту (WCF). Віртуальні локальні мережі (VLAN). Технологія перетворення мережевих адрес (NAT). Захищений периметр. Міжмережеві екрани (МЕ): класифікація та функції МЕ. Варіанти виконання МЕ. Схеми мережевого захисту на базі МЕ. Основні схеми підключення МЕ. Персональні і розподілені мережеві екрани. Довірена мережа та DMZ мережі. Приклади сучасних міжмережевих екранів Тенденції розвитку міжмережевих екранів.

Список рекомендованих джерел:

Основний: 3,4,5
Додатковий: 7, 12-14

Internet-ресурси: 15,18,19,20

Тема 9. Протоколи захисту в телекомунікаційних мережах

Протоколи захисту на канальному рівні (протокол PPTP, L2TP). Протоколи формування захищених каналів на сеансовому рівні (протоколи SSL/TLS, SOCKS). Захист на мережевому рівні (протокол IPSec). Особливості реалізації засобів IPSec. Основні схеми застосування IPSec. Протоколи захисту у бездротових мережах. Механізм шифрування WEP. Специфікація WPA. Стандарт мережі з підвищеною безпекою WPA2.

Список рекомендованих джерел:

Основний: 3,4,5

Додатковий: 7, 12-14

Internet-ресурси: 15,18,19,20

Тема 10. Безпечна робота в комп'ютерних мережах

Віртуальні захищені мережі VPN. Аналіз загроз мережевої безпеки. Види, функції та особливості роботи міжмережевих екранів. Конфігурування міжмережевих екранів. Класифікація та варіанти архітектури мереж VPN. Засоби захисту мереж VPN. Дослідження системи захищеного електронного листування PGP. Захист Wi-Fi мереж. Безпека бездротових мереж. Погрози і ризики безпеки бездротових мереж. Протоколи безпеки бездротових мереж.

Список рекомендованих джерел:

Основний: 2,3,4,5

Додатковий: 6, 9,12,14

Інтернет-джерела: 15, 17-20

5. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

1. Положення про технічний захист інформації в Україні від 27 вересня 1999 року № 1229/99.
2. Остапов С.Е., Євсеєв С.П., Король О.Г., Технології захисту інформації. Навчальний посібник. Чернівці.- Видавничий дім «Родовід», 2014. – 471с.
3. Кавун С.В. Інформаційна безпека: підручник. Харків : ХНЕУ, 2013. -213с.
4. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах: навч. посібник. – К., 2013. – 435с., іл.160.
5. Єсін В. І. Безпека інформаційних систем і технологій: навчальний посібник / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х. : ХНУ імені В. Н. Каразіна, 2013. – 632с.

Додатковий

6. Концепція (основи державної політики) національної безпеки України від 21 грудня 2000 року №2171-111.
7. Інструкція про порядок обліку і зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави від 27 листопада 1998 року № 1893.
8. Положення про порядок здійснення криптографічного захисту інформації в Україні від 22 травня 1998 року № 505/98.
9. Антонюк А., Жора В. Моделювання доступу та каналів витоку в інформаційних системах/Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2014. - №3.160 С.
10. *Пашкова А. Т. Інформаційна безпека як складова національної безпеки А. Т. Пашкова // Безпека життєдіяльності. – Київ, 2014. – № 11. – С. 34-36.*
11. *Полянська В. Кібернетична безпека України в умовах розвитку глобальної інформаційної системи / В. Полянська // Підприємництво, господарство і право. – Київ, 2013. – № 7 (211). – С. 48-50.*
12. A.Menezes, P. van Oorshot, S.Vanstone. Handbook of Applied Cryptography. CRC Press Inc, 2015, 780 p.
13. Г.В.Кузнецов, В.В.Фомичов, С.О.Сушко. Математичні основи криптографії: Ч.1. Дніпропетровськ: Національний гірничий університет, 2014,391с.
14. В.С. Сідак, В.Ю. Артемов. Забезпечення інформаційної безпеки в країнах НАТО та ЄС. К. КНТ. 2012, 160с.

Internet-ресурси

15. Защита информации – режим доступу: *http://www.bseu.by/it/tohod/lekcii9_2.htm*

16.Захист інформації – режим доступу: *http://www.warning.dp.ua/tel28.htm*

*17.*Безпека на прикладному рівні – режим доступу: *http://www.dut.edu.ua*

18. IEEE computer society. SWEBOK – режим доступу: *http://www.computer.org/portal/web/swebok/htmlformat*

19. Process Models in Software Engineering – режим доступу: *http://www.ics.uci.edu/~wscacchi/Papers/SE-Encyc/Process-Models-SE-Encyc.pdf*

20. Technical writing for software engineers – режим доступу: *http://www.dtic.mil/dtic/tr/fulltext/u2/a223872.pdf*

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