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 КНТЕУ

(пост. п. 9 від "23" 12 2021 р.)

Ректор

_____ А.А. Мазаракі

БІОМЕТРИЧНІ ТЕХНОЛОГІЇ АУТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ/

BIOMETRIC AUTHENTICATION TECHNOLOGIES IN INFORMATION SYSTEMS

ПРОГРАМА/

COURSE SUMMARY

Київ 2021

Автори: І.А. ТЕРЕЙКОВСЬКИЙ, доктор технічних наук, професор кафедри інженерії програмного забезпечення та кібербезпеки
В.Я. РАССАМАКІН, кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки
А.О. ФЕСЕНКО, кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Ю.О. САМОЙЛЕНКО, кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібезбезпеки

Програму розглянуто і затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки 1 листопада 2021 р., протокол № 1.

Рецензенти: Н.О. КОТЕНКО, канд. пед. наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки,
Б.Т. БЕБЕШКО, Senior Software Engineer Softorino Ltd.

БІОМЕТРИЧНІ ТЕХНОЛОГІЇ АУТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ/
BIOMETRIC AUTHENTICATION TECHNOLOGIES IN INFORMATION SYSTEMS

ПРОГРАМА/
COURSE SUMMARY

ВСТУП

Дисципліна «Біометричні технології аутентифікації в інформаційних системах» є вибірковою дисципліною навчальних планів підготовки студентів денної форми навчання освітнього ступеня «магістр» галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека» спеціалізації «Безпека систем електронних комунікацій в економіці».

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

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 дисципліни «Біометричні технології аутентифікації в інформаційних системах» є вивчення основних положень сучасних біометричних технологій, опанування методології та методів створення біометричних систем автентифікації, що дозволяють підвищити надійність функціонування складних інформаційних систем.

Завданням дисципліни є: вивчення та розуміння основних концепцій та сучасних теоретичних та практичних проблем проектування біометричних систем аутентифікації, нормативно-правового забезпечення в області технологій біометричного захисту, опанування методології побудови та застосування систем біометричного захисту, математичного забезпечення технологій біометричного захисту, методів застосування згорткових нейронних та рекурентних нейронних мереж, існуючих підходів до застосування нейромережевих моделей та методів для аналізу біометричних параметрів, характеристик систем біометричного захисту.

Предметом вивчення дисципліни є біометричні системи аутентифікації в інформаційних системах.

2. ПЕРЕДУМОВИ ВИВЧЕННЯ ДИСЦИПЛІНИ ЯК ВИБІРКОВОЇ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ

Знання та вміння здобуті у результаті вивчення дисциплін «Методи і засоби захисту інформації в комп'ютерних системах», «Хмарні та GRID-технології», «Функціональне та логічне програмування», «Enterprise програмування Jawa», «Технології проектування інформаційних систем», «Англійська мова інформаційних технологій».

3. РЕЗУЛЬТАТИ ВИВЧЕННЯ ДИСЦИПЛІНИ

Дисципліна «Біометричні технології аутентифікації в інформаційних системах», як вибіркова 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, ОП 2022р.)

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-2	Здатність проводити дослідження на відповідному рівні.	1-12
КЗ-3	Здатність до абстрактного мислення, аналізу та синтезу.	1-12
КЗ-4	Здатність оцінювати та забезпечувати якість виконуваних робіт.	1-12
КЗ-5	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).	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 сфе-	1-12

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
	рі інформаційної безпеки та/або кібербезпеки.	
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
КФ4	Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.	1-12
КФ5	Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес / операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	1-12
КФ6	Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	1-12

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
КФ7	Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.	1-12
Програмні результати навчання		
РН01	Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес \ операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	1-10
РН02	Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.	1-12
РН03	Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	1-12
РН04	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	1-12
РН05	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
РН06	Аналізувати та оцінювати захищеність	1-12

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
	систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	
РН07	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	1-12
РН08	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	1-12
РН09	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	1-12
РН10	Забезпечувати безперервність бізнес / операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	1-12
РН12	Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів 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
РН16	Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із	1-12

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
	застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.	
РН17	Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.	1-12
РН19	Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.	1-12
РН20	Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.	1-12
РН21	Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.	1-12
РН22	Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.	1-12
РН23	Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також 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.	1-12

4. ЗМІСТ ДИСЦИПЛІНИ

Тема 1. Вступ, основні поняття та визначення

Біометрія як наука. Історія розвитку біометричних технологій. Основні визначення в області біометрії. Поняття біометричного параметру. Статичні та динамічні методи біометричної аутентифікації.

Список рекомендованих джерел:

Основний: 2, 3.

Додатковий: 5-7.

Інтернет-ресурси: 8-10.

Нормативно-правові документи: 1,2.

Тема 2. Нормативно-правове забезпечення в області технологій біометричного захисту

Законодавчі основи застосування біометричних технологій. Державні стандарти України в області технологій біометричного захисту. Коротка характеристика вітчизняних нормативних документів в області біометрії. Особливості законодавства США та ЄС в області біометрії.

Список рекомендованих джерел:

Основний: 2,3.

Додатковий: 5, 7.

Інтернет-ресурси: 8,10.

Нормативно-правові документи :1,2.

Тема 3. Методологія побудови та застосування систем біометричного захисту

Структура системи біометричної аутентифікації. Призначення та характеристика основних модулів системи біометричної аутентифікації. Особливості реєстрації статичних та динамічних біометричних параметрів. Проблематика аналізу біометричних параметрів.

Список рекомендованих джерел:

Основний: 1 – 3.

Додатковий: 5-7.

Інтернет-ресурси: 8-10.

Тема 4. Математичне забезпечення технологій біометричного захисту.

Методологія первинної обробки біометричних параметрів. Нормалізація біометричних параметрів. Фільтрація біометричних параметрів. Особливості аналізу біометричних параметрів для розпізнавання особи користувача комп’ютерної системи.

Список рекомендованих джерел:
Основний: 1-3.
Додатковий: 4-7.
Інтернет-ресурси: 8-10.

Тема 5. Підходи до застосування нейромережевих моделей та методів для аналізу біометричних параметрів

Поняття штучної нейронної мережі. Штучний нейрон. Функція активації. Нейронні мережі з прямим розповсюдженням сигналу. Алгоритм зворотного поширення помилки.

Список рекомендованих джерел:
Основний: 1-2.
Додатковий: 4,5,7.
Інтернет-ресурси: 8.

Тема 6. Методи застосування згорткових нейронних мереж

Поняття згорткової нейронної мережі. Структура згорткової нейронної мережі. Процедура згортки. Процедура масштабування. Застосування згорткових нейронних мереж і біометрії.

Список рекомендованих джерел:
Основний: 1-2.
Додатковий: 4,5,7.
Інтернет-ресурси: 8.

Тема 7. Методи застосування рекурентних нейронних мереж

Поняття рекурентної нейронної мережі. Нейронні мережі типу Елмана та Джордана. Нейронна мережа типу LSTM. Нейронна мережа типу GRU. Застосування рекурентних нейронних мереж в біометрії.

Список рекомендованих джерел:
Основний: 1-2.
Додатковий: 4,5,7
Інтернет-ресурси: 8.

Тема 8. Характеристика систем біометричного захисту

Біометрична аутентифікація користувачів комп'ютерних систем. Система контролю і управління доступом в у приміщеннях. Ідентифікація в мобільних пристроях. Електронні системи голосування. Впровадження біометричних розробок.

Список рекомендованих джерел:
Основний: 1-3.
Додатковий: 5-7.
Інтернет-ресурси: 8-10.

Тема 9. Біометрична ідентифікація за допомогою відбитків пальців

Характеристика відбитків пальців. Класифікація відбитків пальців. Методи та класифікатори автоматизованої класифікації відбитків пальців. Алгоритми ідентифікації відбитків у рамках обраного класу. Пристрої для отримання відбитків пальців в електронному вигляді.

Список рекомендованих джерел:

Основний: 2.

Додатковий: 5-7.

Інтернет-ресурси: 8,10.

Тема 10. Ідентифікація на основі параметрів геометрії ока та за допомогою голосу

Ідентифікація на основі параметрів ока. Методи розпізнавання на основі райдужної оболонки ока. Проблеми ідентифікації на основі райдужної оболонки ока. Характеристика голосу. Алгоритми голосової ідентифікації. Методи та механізми голосової ідентифікації. Порівняння механізмів голосової ідентифікації.

Список рекомендованих джерел:

Основний: 2.

Додатковий: 5-7.

Інтернет-ресурси: 8,10.

Тема 11. Біометрична ідентифікація за клавіатурним почерком

Ідентифікація за параметрами почерку. Алгоритми ідентифікації за параметрами почерку. Ідентифікація користувачів за клавіатурним почерком на базі параметричного вивчення класифікатора.

Список рекомендованих джерел:

Основний: 2.

Додатковий: 5-7.

Інтернет-ресурси: 8,10.

Тема 12. Огляд поширених систем біометричної ідентифікації

Система біометричної ідентифікації BioLink IDenium. Система біометричної ідентифікації АДИС ПАПИЛО. Система ідентифікації VOCORD FaceContro. Система ідентифікації EyeSwipe Nano. Система ідентифікації Smilart. Система ідентифікації Face-Інспектор.

Список рекомендованих джерел:

Основний: 2.

Додатковий: 5-7.

Інтернет-ресурси: 8,10.

5. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

1. Корченко О. Методологія розроблення нейромережевих засобів інформаційної безпеки Інтернет-орієнтованих інформаційних систем: навч. посіб. / О. Корченко, І. Терейковський, А. Білощицький. – К. : ТОВ «Наш Формат». – 2016. – 249 с.
2. Царьов Р.Ю. Біометричні технології: навч. посіб. [для вищих навчальних закладів] / Р.Ю. Царьов, Т. М. Лемеха. – Одеса: ОНАЗ ім. О.С. Попова, 2016. – 140 с.: іл.
3. *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.*

Додатковий

4. Корченко А. Нейросетевые модели, методы и средства оценки параметров безопасности Интернет-ориентированных информационных систем: монографія / А. Корченко, И. Терейковский, Н. Карпинский, С. Тынымбаев. – К. : ТОВ «Наш Формат». – 2016. – 275 с.
5. Кумченко Ю.О. Інформаційна технологія ідентифікації персоналу на основі комплексу біометричних параметрів Дисертація на здобуття наукового ступеня кандидата технічних наук 05.13.06 – Інформаційні технології ДВНЗ «Криворізький національний університет», 2017 р. – 145 с.
6. Прудник А. М. Биометрические методы защиты информации / А. М. Прудник, Г. А. Власова, Я. В. Рощупкин. – 2014. – 123 с.
7. Фесенко А.О. Методи обробки даних для систем ідентифікації та аутентифікації на основі біометричних характеристик ока. Автореферат дисертації на здобуття наукового ступеня кандидата технічних наук – Київ, «НВФ «Славутич-Дельфін». 2017 р. – 21 с.

Інтернет-ресурси

8. Засоби і методи біометричної автентифікації користувачів в комп'ютерних системах – Режим доступу: http://poteme.com.ua/informatika/stati-po-informatike/1653-zasobi-i-metodi-biometrichnoji-autentifikatsiji-koristuvachiv-v-komp-yuternikh-sistemakh.html
9. Ідентифікація та аутентифікація – Режим доступу: https://sites.google.com/site/identifikaciataautentifikacia/ponatta-pro-autentifikaciu/metodi-autentifikaciie

10. Засоби захисту інформації – Режим доступу: http://allref.com.ua/uk/skachaty/Zasobi_zahistu_informaciyi?page=7
11. Біометричні системи автентифікації на базі SDK (Intel Perceptual Computing) – Режим доступу: https://ppt-online.org/102808
12. Використання нейронних мереж з прямим розповсюдженням сигналу для розпізнавання скриптового шкідливого програмного забезпечення– Режим доступу: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Nzundiz_2015_2_12
13. Deep Convolutional Neural Network (DCNN) – Режим доступу: https://proceedings.neurips.cc/paper/2014/file/1c1d4df596d01da60385f0bb17a4a9e0-Paper.pdf
14. Кваліфікований електронний підпис – Режим доступу: https://dmsu.gov.ua/faq/kvalifikovanij-elektronnij-pidpis-kep.html
15. Хмарна система контролю доступом. Режим доступу - https://www.samekey.com/?lang=uk&gclid=EAIaIQobChMI84Xtg4HR8wIVweeyCh0Mrw4IEAAYASAAEgICAvD_BwE
16. Системи контролю та управління доступом. Режим доступу: https://smartsec.com.ua/uk/produkti/sistemy-kontrolyu-ta-upravlinnya-dostupom/

Нормативно-правові документи

1. Про інформацію : Закон України прийнятий Верховною Радою України 06.10.2000 № 1642-III (зі змін. та доповн.). – Режим доступу : https://zakon.rada.gov.ua/laws/show/2657-12#Text
2. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України прийнятий Верховною Радою України 05.07.1994 № 80/94-ВР (зі змін. та доповн.). – Режим доступу : https://zakon.rada.gov.ua/laws/show/80/94-вр#Text

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