

**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 програмної інженерії та кібербезпеки

ЗАТВЕРДЖЕНО

вченою радою

(пост. п. ___ від "___" _____ 201_ р.)

Ректор

_____ А.А. Мазаракі

**СИЛАБУС
БІОМЕТРИЧНІ ТЕХНОЛОГІЇ АУТЕНТИФІКАЦІЇ
В ІНФОРМАЦІЙНИХ СИСТЕМАХ
BIOMETRIC AUTHENTICATION TECHNOLOGIES IN
INFORMATION SYSTEMS
SYLLABUS**

освітній ступінь

магістр / master

галузь знань

**12 Інформаційні технології / Information
Technology**

спеціальність

**121 Інженерія програмного
забезпечення / Software Engineering**

спеціалізація

**Інженерія програмного забезпечення /
Software Engineering**

*Гарант освітньо-
професійної програми
"Інженерія програмного
забезпечення" другого
(магістерського) рівня
вищої освіти*

*Завідувач
кафедри про-
грамної ін-
женерії та
кібербезпеки,
д.т.н., проф.
Дриворукко О.В.*

Київ 2019

Розповсюдження і тиражування без офіційного дозволу КНТЕУ заборонено

Автори: Рассамакін В. Я., канд. техн. наук, доц.
Терейковський Ігор Анатолійович, доктор техн наук,
професор

Силабус розглянуто і затверджено на засіданні кафедри програмної інженерії та кібербезпеки 10 вересня 2019 р., протокол № 3

СИЛАБУС

БІОМЕТРИЧНІ ТЕХНОЛОГІЇ АУТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

BIOMETRIC AUTHENTICATION TECHNOLOGIES IN INFORMATION SYSTEMS

SYLLABUS

освітній ступінь	магістр / master
галузь знань	12 Інформаційні технології / Information Technology
спеціальність	121 Інженерія програмного забезпечення / Software Engineering
спеціалізація	Інженерія програмного забезпечення / Software Engineering

АНОТАЦІЯ КУРСУ

1. Викладачі:

1.1. **Лектор:** Терейковський Ігор Анатолійович.

- доктор техн. наук, професор кафедри програмної інженерії та інформаційних систем КНТЕУ (Київський політехнічний інститут імені Ігоря Сікорського професор кафедри системного програмування та спеціалізованих комп'ютерних систем);
- *педагогічний стаж* – 22 роки;
- *контактний телефон:* +38(067)909-58-67;
- *e-mail:* terejkowski@ukr.net

–*наукові інтереси:* нейронні мережі в засобах захисту комп'ютерної інформації; захист інформації в комп'ютерних системах; розвиток теоретичного підґрунтя підвищення ефективності захисту інформації в комп'ютерних системах та мережах методів за рахунок застосування методів штучного інтелекту та спектрального аналізу.

– *стажування та підвищення кваліфікації:* у період з 1.05.18 по 31.05.18 в рамках програми Горизонт 2020 пройшов стажування в Інституті обчислювальної та прикладної математики ім. Й.Радона Австрійської академії наук у м. Лінц. (Certificate of the Johann Radon Institute, Linz, May, 2018)

1.2. **Ассистент лектора:** Рассамакін Володимир Якович,

- к.т.н., доцент кафедри програмної інженерії та кібербезпеки;
- *педагогічний стаж* – 22 роки;
- *контактний телефон:* +38(050)190-70-99;
- *e-mail:* rassamakin_vr@knute.edu.ua
- *наукові інтереси:* Інформаційні системи і технології, апаратне забезпечення комп'ютерної техніки та сучасна елементна база ЕОМ.
- *стажування та підвищення кваліфікації:*
 - Корпорація ПАРУС м. Київ, сертифікат за № 14526421 тема: «Парус Підприємство 7.40» CRM-модуль «Менеджмент-маркетинг», 08.02.12.;
 - ТОВ «Інтелект Сервіс» м. Київ, сертифікат № ТЕУ/П 0025 на право викладання та придбання програми «М.Е.Дос», тема: «Теоретично-практичний курс по роботі з комп'ютерною програмою М.Е.Дос для права її викладати на навчальних курсах», 26.11.15.
 - Навчальний центр «Успіх» м. Київ сертифікат № 01.01.16 за програмою «Менеджер комп'ютерних систем», 19.02.16;
 - ТОВ «БіДжіЕс Консалтінг» сертифікат № А-00024 тема: «ІС:Підприємство» модуль «Технології програмування та конфігурація на платформі «ІС:Підприємство 8», 30.01.17;
 - ТОВ «Майкрософт Україна» (м. Київ), сертифікат №ДО751814 успішно пройденого курсу підвищення кваліфікації, тема:

«Використання хмарних сервісів Microsoft в освітньому процесі»,
09.11.18.

2. Дисципліна: «БІОМЕТРИЧНІ ТЕХНОЛОГІЇ АУТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ»,

- рік навчання: II
- семестр навчання: III
- кількість кредитів: 6
- кількість годин за семестр: 180
 - лекційних: 14
 - лабораторних: 28
 - на самостійне опрацювання: 138
- кількість аудиторних годин на тиждень:
 - лекційних: 2
 - лабораторних: 4

3. Час та місце проведення:

- аудиторні заняття - відповідно до розкладу КНТЕУ з врахуванням специфіки дисципліни передбачено аудиторія: 504, 510, 510а, 514;
- поза аудиторна робота - самостійна робота студента, результат виконання якої висвітлено засобами Office 365

4. Пререквізити та постреквізити навчальної дисципліни:

- **пререквізити:** «Об'єктно-орієнтоване програмування», «Архітектура та проектування програмного забезпечення», «Архітектура комп'ютера», «Алгоритми та структури даних», «Людино-машинна взаємодія», «Технології проектування інформаційних систем», «Методи і засоби захисту інформації в комп'ютерних системах».
- **постреквізити:**
У результаті вивчення навчальної дисципліни студенти повинні **знати** (компетентності):
 - основні поняття і визначення, історія розвитку біометричних технологій;
 - законодавчі та правові основи захисту комп'ютерної інформації та інформаційних технологій;
 - сучасні біометричні системи захисту, їх взаємодію з іншими системами;
 - групи систем за типом використовуваних біометричних параметрів;
 - методи автентифікації біометричних систем;
 - сучасні біометричні технології;
 - види біометричних технологій. Позитивні і негативні сторони застосування кожної технології;

- застосування біометричних технологій для захисту сучасних систем передачі даних;
- області застосування біометричних систем.

вміти:

- оцінювати переваги і недоліки кожного з видів біометричних технологій;
- здійснювати аналіз технічної задачі для вибору одного (оптимального) методу біометричного захисту;
- визначати можливості комбінації біометричних технологій для більш повноцінного захисту інформації.

володіти:

- - уявленнями про проектування біометричних систем аутентифікації.

5.Характеристика дисципліни:

5.1.Призначення навчальної дисципліни: набуття студентами знань щодо існуючих технологій біометричного захисту інформації, визначення переваг і недоліків кожної технології, отримання практичних навичок з аналізу технічної задачі для вибору оптимального методу біометричного захисту, можливостей комбінації технологій для більш повноцінного захисту

5.2.Мета вивчення дисципліни: вивчення основних положень сучасних біометричних технологій, опанування методів та методологій створення біометричних систем аутентифікації, що дозволяють підвищити надійність функціонування складних інформаційних систем

5.3.Задачі вивчення дисципліни: є:

- вивчення та розуміння основних концепцій та сучасних теоретичних та практичних проблем проектування біометричних систем аутентифікації, зокрема вибору системи інформативних ознак, формування векторів ознак і методу їх порівняння;
- оволодіння існуючими статичними біометричними методами та ознайомлення з динамічними методами біометричної аутентифікації;
- оволодіння відомими алгоритмами розпізнавання мовних сигналів в голосових системах біометричної аутентифікації, особливостями дактилоскопічних зображень та існуючих алгоритмів і методів попередньої обробки цих зображень, систем інформативних ознак та методів їх порівняння; моделювання спотворень дактилоскопічних зображень та створення біометричної ідентифікаційної системи.

5.4.Зміст навчальної дисципліни: відповідає навчальній та робочій програмі, визначеній науковими досягненнями як наукові досягнення вітчизняних та закордонних вчених, а також запитам стейкхолдерів.

5.5. План вивчення дисципліни

Результати навчання	Навчальна діяльність	Робочий час студента (год.)	Оцінювання (бал)
1	2	3	4
Тема 1. Вступ, основні поняття та визначення		38	25
<p>Знати історичні аспекти розвитку, основні поняття та визначення біометрії, біометричних технологій, законодавчі і нормативні акти застосування біометричних технологій.</p> <p>SoftSkills: комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики, колективний тайм менеджмент</p>	<p>Лекція 1. Вступ, основні поняття та визначення</p> <p>План лекції:</p> <ol style="list-style-type: none"> 1. Біометрія як наука. 2. Історія розвитку біометричних технологій. 3. «Законодавчі і правові основи захисту комп'ютерної інформації та інформаційних технологій». 4. Законодавчі основи застосування біометричних технологій. 5. Правові засади застосування біометричних технологій в захисті інформації. <p>Список рекомендованих джерел: Нормативно-правові документи :1,2. Основний: 1 – 4. Додатковий: 5, 6. Інтернет-ресурси: 8, 9</p>	2	
	<p>Завдання для самостійної роботи: Вивчення та доповнення матеріалів лекції на основі самостійного опрацювання основних літературних джерел, зазначених у списку та електронних матеріалів, які надаються викладачем.</p> <p>Питання винесені на самостійне опрацювання:</p> <ol style="list-style-type: none"> 1. Проблеми точності біометричної ідентифікації в історії розвитку методів контролю доступу до інформації 2. Законодавчі та правові основи захисту комп'ютерної інформації та інформаційних технологій 	30	4
<p>Вміти синтезувати і виконувати аналіз проектних рішень щодо забезпечення безпеки інформаційних систем, використовувати існуючі</p>	<p>Лабораторні заняття №1 «Інтеграція можливостей модулів Intel Perceptual Computing SDK для реалізації багаторівневої системи інформаційної безпеки, заснованої на біометричній інформації »</p> <p><i>Мета: Ознайомлення з біометричними системами інформаційної безпеки на основі Intel Perceptual Computing SDK</i></p> <p>План заняття:</p> <ol style="list-style-type: none"> 1. Ознайомлення з основними термінами і принципами роботи з SDK (software 	2	7

1	2	3	4
<p>програмні засоби інформаційної безпеки на основі біометричних методів</p>	<p>development kit).</p> <p>2. Дослідження можливостей модулів Intel Perceptual Computing SDK.</p> <p>3. аналіз проведеної роботи.</p> <p>Лабораторні заняття №2 «Методи ідентифікації особистості по райдужній оболонці ока» <i>Мета: Вивчити основні методи аутентифікації по райдужній оболонці ока і принципи функціонування таких систем</i></p> <p>План заняття:</p> <p>1. Вивчити типи, види, програмні засобами для ідентифікації особистості по райдужній оболонці ока.</p> <p>2. Детальне вивчення принципу роботи методу та виконання практичного завдання.</p> <p>Лабораторні заняття №3 «Актуальні методи ідентифікації особистості». <i>Мета: Вивчення способів ідентифікації особистості за її біометричними параметрами.</i></p> <p>План заняття:</p> <p>1. Проаналізувати історія розвитку та вивчити принципи роботи методу захисту інформації по зображенню особи у візуальному і інфрачервоному діапазонах спектру.</p> <p>2. Проаналізувати історія розвитку та вивчити принципи роботи методу аудіо захисту інформації.</p> <p>3. Вивчити типи, види, програмні засоби для ідентифікації особистості по відбитку пальців.</p> <p>4. Вивчити типи, види, програмні засоби для ідентифікації особистості по геометрії обличчя особи.</p> <p>5. Докладне вивчення принципів роботи методів та виконання практичного завдання</p>	<p>2</p> <p>2</p>	<p>7</p> <p>7</p>
<p>Тема 2. Сучасні біометричні системи захисту. Взаємодія з іншими системами</p>		<p>44</p>	<p>25</p>
<p>Знати: існуючу класифікацію груп та методів біометричних систем захисту,</p>	<p>Лекція №2 Групи систем за типом використовуваних біометричних параметрів. План лекції:</p> <p>1. Статичні методи біометричної аутентифікації</p> <p>2. Динамічні методи біометричної</p>	<p>2</p>	

1	2	3	4
<p>сучасні принципи, апаратні та програмні, засоби технологій біометричної ідентифікації та аутентифікації.</p> <p>SoftSkills: комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики, колективний тайм менеджмент</p>	<p>аутентифікації</p> <p>3. Комбіновані методи біометричної аутентифікації</p> <p>Список рекомендованих джерел: Основний: 1 – 4. Додатковий: 5, 6. Інтернет-ресурси: 9.</p> <p>Лекція №3 Характеристика методів аутентифікації біометричних систем.</p> <p>План лекції:</p> <p>1. Біометричні методи ідентифікації 2. Біометричні методи верифікації</p> <p>Список рекомендованих джерел: Основний: 1 – 4. Додатковий: 5, 6. Інтернет-ресурси: 9.</p>	2	
<p>Вміти: визначати переваги і доцільність застосування біометричних засобів ідентифікації, володіти статистичними і динамічними методами біометричної аутентифікації з використанням сучасних програмно-апаратних засобів.</p>	<p>Завдання для самостійної роботи: Вивчення та доповнення матеріалів лекції на основі самостійного опрацювання основних літературних джерел, зазначених у списку та електронних матеріалів, які надаються викладачем.</p> <p>Питання винесені на самостійне опрацювання:</p> <p>1. Сучасні сканери біометричних даних. 2. Поведінкова аутентифікація користувачів.</p>	36	5
	<p>Лабораторне заняття №4 «Статистичні методи біометричної аутентифікації»</p> <p>Мета: Вивчення статистичних методів біометричної аутентифікації</p> <p>План заняття:</p> <p>1. Огляд існуючих методів розпізнавання обличчя. 2. Створення моделі обличчя з використанням в модулів Intel Perceptual Computing SDK в інтерактивній формі. 2. Кореляційне порівняння відбитків пальців. 3. Типу, види, область застосування ідентифікаторів за відбитками пальців. 4. Розпізнавання відбитків пальців засобами Python</p> <p>Лабораторне заняття №5 «Динамічні методи біометричної аутентифікації»</p>	2	10

1	2	3	4
	<p><i>Мета: Вивчення динамічних методів біометричної аутентифікації</i></p> <p>План заняття:</p> <ol style="list-style-type: none"> 1. Розгляд методів захисту інформації за підписом. 2. Біометричні методи захисту інформації по голосу (аудіо): типи, види, програмні засоби для ідентифікації особистості по голосу. 3. Розпізнавання мови з використанням можливостей модулів Intel Perceptual Computing SDK » 4. Біометричні методи захисту інформації по клавіатурного почерку 	2	10
Тема 3. Сучасні біометричні технології.		48	25
<p>Знати основні види біометричних технологій заснованих на біометричних характеристиках ідентифікації людини.</p> <p>Вміти: обирати методи і засоби захисту інформації біометричними методами, використовувати пакети обробки і аналізу експериментальних даних, узагальнювати і інтерпретувати отримані результати</p> <p>SoftSkills: комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики.</p>	<p>Лекція 4. Види біометричних технологій, їх позитивні і негативні сторони застосування.</p> <ol style="list-style-type: none"> 1. Автоматизована дактилоскопічна ідентифікаційна система. 3. Система ідентифікації по рукописному почерку. <p>Список рекомендованих джерел: Основний: 1 – 4. Додатковий: 5, 6. Інтернет-ресурси: 7, 8.</p> <p>Лекція 5. Інтеграція біометричних технологій з системами захисту підприємства. (в інтерактивній формі)</p> <ol style="list-style-type: none"> 1. Застосування біометричних технологій в системах відео спостереження. 2. Застосування біометричних технологій в системах контролю доступу персоналу 3. Застосування біометричних технологій в інших сучасних системах <p>Список рекомендованих джерел: Основний: 1 – 4. Додатковий: 5, 6. Інтернет-ресурси: 7, 8.</p> <p>Завдання для самостійної роботи: Вивчення та доповнення матеріалів лекції на основі самостійного опрацювання основних літературних джерел, зазначених у списку та електронних матеріалів, які надаються викладачем.</p> <p>Питання винесені на самостійне опрацювання:</p> <ol style="list-style-type: none"> 1. Комбіновані методи біометричної аутентифікації. 2. Автоматизована дактилоскопічна ідентифікаційна система 	<p>2</p> <p>2</p> <p>36</p>	<p>3</p>

1	2	3	4
	<p>Лабораторне заняття № 6 <i>Мета: Вивчення оптимальних систем захисту.</i></p> <p>План заняття:</p> <ol style="list-style-type: none"> 1. Вибір оптимальної системи доступу до банківської інформації 2. Вибір оптимальної системи доступу до окремих приміщень. 3. Застосування біометричних технологій при використанні електронного цифрового підпису. 4. Вибір оптимальної системи захисту ЕЦП. 	2	5
	<p>Лабораторне заняття № 7 <i>Мета: Вивчення сучасних програмних засобів біометричних технологій.</i></p> <p>План заняття:</p> <ol style="list-style-type: none"> 1. Комбіновані методи біометричної аутентифікації. 2. Види комп'ютерних атак на біометричні системи, способи їх виявлення. 	2	5
	<p>Лабораторне заняття № 8 <i>Мета: Вивчення основних напрямків розвитку біометричних технологій в сучасному середовищі.</i></p> <p>План заняття:</p> <ol style="list-style-type: none"> 1. Контроль і облік робочого часу співробітників підприємства за допомогою біометричних технологій. 2. Контроль доступу користувачів інформації автоматизованих систем за допомогою біометричних технологій. 3. Основні законодавчі та нормативні акти для застосування біометричних технологій. 4. Перспективи біометричних систем безпеки в Україні. 	2	6
	<p>Лабораторне заняття № 9 <i>Мета: Докладне вивчення властивостей біометричних параметрів.</i></p> <p>План заняття:</p> <ol style="list-style-type: none"> 1. Вимірюваність біометричних параметрів. 2. Приємливість біометричних параметрів. 3. Автоматична ідентифікація. 4. Формати обміну біометричними даними. 	2	
Тема 4. Области застосування біометричних систем.		50	25
Знати існуючі і перспективні області	<p>Лекція 6. Области застосування біометричних систем. Проблеми впровадження біометричних технологій.</p> <ol style="list-style-type: none"> 1. Система контролю і управління доступом в 	2	

1	2	3	4
<p>застосування методів біометричного захисту інформації</p> <p>SoftSkills: комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики.</p>	<p>приміщеннях.</p> <p>2. Ідентифікація в мобільних пристроях</p> <p>3. Електронні системи голосування</p> <p>4. Впровадження біометричних розробок.</p> <p>Список рекомендованих джерел: Основні: 1 – 4. Додаткові: 5, 6. Інтернет-ресурси: 7, 8</p> <p>Лекція 7. Застосування біометричних технологій для захисту сучасних систем передачі даних.</p> <p>1. Біометричні технології в системах передачі даних.</p> <p>2. Захист біометричних технологій в системах передачі даних.</p> <p>Список рекомендованих джерел: Основні: 1 – 4. Додаткові: 5, 6. Інтернет-ресурси: 7, 8</p> <p>Завдання для самостійної роботи: Вивчення та доповнення матеріалів лекції на основі самостійного опрацювання основних літературних джерел, зазначених у списку та електронних матеріалів, які надаються викладачем.</p> <p>Питання винесені на самостійне опрацювання:</p> <p>1. Основні компанії, представлені на ринку, вибір оптимального обладнання та програмного забезпечення за напрямками.</p> <p>2. Основні напрямки розвитку біометричних технологій на сучасному етапі</p>	<p>2</p> <p>36</p>	<p>2</p>
<p>Вміти визначати перспективні напрямки розвитку біометричних технологій, використовувати засоби усунення помилок та захисту біометричних систем</p>	<p>Лабораторне заняття № 10 <i>Мета: Вивчення систем обліку робочого часу на підприємстві.</i></p> <p>План заняття.</p> <p>1. Вибір оптимальної системи обліку робочого часу підприємства.</p> <p>2. Контроль обліку робочого часу підприємства.</p> <p>Лабораторне заняття № 11 <i>Мета: Вивчення існуючих розробок біометричних систем компаніями</i></p> <p>План заняття.</p> <p>1. Основні компанії, представлені на ринку, вибір оптимального обладнання та програмного забезпечення за напрямками.</p> <p>2. Відмінності продукцій обладнання і програмного забезпечення по напрямками</p>	<p>2</p> <p>2</p>	<p>4</p> <p>4</p>

1	2	3	4
	<p>Лабораторне заняття № 12 <i>Мета: вивчення способів усунення помилок ідентифікації, запобігання атак на систему введення</i></p> <p>План заняття</p> <ol style="list-style-type: none"> 1. Аналіз типових помилок систем 2. Вибір оптимальних варіантів для усунення помилок. 3. Захист від примусової атаки 4. Захист від імітаційної атаки 5. Захист від атаки відтворення 	2	6
	<p>Лабораторне заняття № 13 <i>Мета: вивчення архітектури та характеристик біометричних систем аутентифікації</i></p> <p>План заняття</p> <ol style="list-style-type: none"> 1. Коефіцієнт помилкових відмов і помилкових підтверджень, архітектура біометричних систем аутентифікації. 2. Самонавчання біометричних систем. 	2	4
	<p>Лабораторне заняття № 14 <i>Мета: вивчення методу біометричної аутентифікація користувача по клавіатурного почерку</i></p> <p>План заняття</p> <ol style="list-style-type: none"> 1. Дослідження біометричних підсистем ідентифікації та аутентифікації користувачів на прикладі розгляду програмного комплексу аналізу динаміки роботи користувача на клавіатурі. 2. Навчання біометричної системи, розпізнавання користувачів, визначення коефіцієнтів помилкових відмов і помилкових підтверджень 	2	5
Разом		180	100
Підсумковий контроль		Письмовий екзамен	

6. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Нормативно-правові документи

1. Про інформацію: Закон України від 02.10.1992 № 2658-ХІІ (зі змін. та доповн.) // Відомості Верховної Ради України. – 1992. -№ 48
2. Про захист інформації в автоматизованих системах : Закон України від 05.07.1994 № 81/94-ВР// Відомості Верховної Ради України. -1994. -№ 31.

Основний

1. Прудник А. М. Биометрические методы защиты информации / А. М. Прудник, Г. А. Власова, Я. В. Рощупкин. – Минск: БГУИР, 2014. – 123 с
2. Русин Б.П. Біометрична аутентифікація та криптографічний захист./ Б.П.Русин, Я.Ю.Варецький - Львів: Коло, 2007. - 287 с.
3. Традиционные методы биометрической аутентификации и идентификации : навчальний електронний посібник / Колешко В. М., Воробей Е. А., Азизов П. М. [та ін.]. – Минск : БНТУ, 2009. – 107 с. –
4. Хорошко В.О., Х 80 Основи інформаційної безпеки / В.С.Чередниченко, М.Є Шелест, За ред. проф. В.О. Хорошка. - К.: ДУІКТ, 2008.- 186 с..

Додатковий

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. Фабричнов А.Г., Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник / Н.Н Куняев., А.С.Дёмушкин - Киев, Логос, 2011 г. 448 с..

Интернет-ресурси

7. Засоби і методи біометричної аутентифікації користувачів в комп'ютерних системах – Режим доступу: <http://portal.com.ua/informatika/stati-po-informatike/1653-zasobi-i-metodi-biometrichnoji-autentifikatsiji-koristuvachiv-v-komp-yuternikh-sistemakh.html>
8. Ідентифікація та аутентифікація – Режим доступу: <https://sites.google.com/site/identifikaciataautentifikacia/ponatta-pro-autentifikaciu/metodi-autentifikacii>
9. Засоби захисту інформації – Режим доступу: http://allref.com.ua/uk/skachaty/Zasobi_zahistu_informaciyi?page=7

7. **Контроль та оцінювання результатів навчання:** положення про оцінювання результатів навчання студентів і аспірантів наказ КНТЕУ №2891 від 16.09.2019р.

Під час вивчення дисципліни «Проектування мультимедійних систем» викладачем здійснюється поточний та підсумковий контроль. Поточний контроль та оцінювання передбачає:

- перевірку рівня засвоєння теоретичного матеріалу (тестування за матеріалами лекції, який здійснюється на початку кожної наступної лекції з використанням 365 Office);
- захист лабораторних робіт (проходить під час наступної лабораторної роботи);
- перевірка засвоєння матеріалу, що винесений на самостійне опрацювання під час фронтального опитування на лекції.

8. Політика навчальної дисципліни:

8.1. Відвідування лекційних та лабораторних занять: відвідування лекційних та лабораторних занять є обов'язковим. Допускаються пропуски занять з таких поважних причин, як хвороба (викладачу надається копія довідки від медичного закладу), участь в олімпіаді, творчому конкурсі тощо за попередньою домовленістю та згодою викладача за умови дозволу деканату (надаються документи чи інші матеріали, які підтверджують заявлену участь у діяльності студента).

8.2. Відпрацювання пропущених занять: відпрацювання пропущених занять є обов'язковим незалежно від причини пропущеного заняття. Лекційне заняття має бути відпрацьоване до наступної лекції на консультації викладача з використанням ПЗ 365 Office Teams. Відпрацювання лекційного матеріалу передбачає вивчення пропущеного теоретичного матеріалу та складання тесту за цим матеріалом. Лабораторне заняття відпрацьовується під час консультації викладача (розклад консультацій на сайті).

8.3 Правила поведінки під час занять: обов'язковим є дотримання техніки безпеки в комп'ютерних лабораторіях. Студенти повинні приймати активну участь в обговоренні навчально матеріалу ознайомившись з ним напередодні (навчальний матеріал надається викладачем).

8.4 За порушення академічної доброчесності студенти будуть притягнені до такої академічної відповідальності:

- повторне проходження оцінювання (контрольна робота, іспит, залік тощо);
- повторне проходження навчального курсу.