ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ АВТОМАТИЗОВАНИХ СИСТЕМ

Семестр	**7**
Освітньо-професійний ступінь	**Фаховий молодший бакалавр**
Кількість кредитів ЄКТС	**3**
Форма контролю	**Залік**
Аудиторні години	**32 (14 год. лекцій, 4 год. практичних, 14 год. лабораторних)**

Загальний опис дисципліни

Дисципліна «Технічні засоби захисту автоматизованих систем» вивчає методи та засоби забезпечення безпеки автоматизованих систем керування (АСК). Розглядаються технічні та програмні механізми захисту від кібератак, фізичного несанкціонованого доступу, техногенних загроз, а також методи резервування та відновлення систем. Особлива увага приділяється криптографічним засобам, системам аутентифікації, контролю доступу та моніторингу безпеки.

Майбутній фахівець повинен мати наступні компетентності:

Інтегральна компетентність	Здатність вирішувати типові спеціалізовані задачі в галузі електроніки, автоматизації та електронних комунікацій у процесі навчання, що вимагає застосування положень і методів відповідних наук та може характеризуватися певною невизначеністю умов; нести відповідальність за результати своєї діяльності; здійснювати контроль інших осіб у визначених ситуаціях.
Загальні компетентності	ЗК3. Здатність застосовувати знання у практичних ситуаціях. ЗК4. Навички використання інформаційних і комунікаційних технологій.
Спеціальні (фахові, предметні) компетентності	СК4. Здатність аргументувати вибір технічних засобів автоматизації на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи автоматизації і експлуатаційних умов; мати навички налагодження та обслуговування технічних засобів автоматизації і систем керування. СК7. Здатність застосовувати новітні технології в галузі автоматизації; використовувати комп'ютерно-інтегровані технології для збору даних та їх архівування; створювати бази даних параметрів процесу та їх візуалізації за допомогою засобів людино-машинного інтерфейсу. СК8. Здатність обґрунтовувати вибір технічної структури та розробляти прикладне програмне забезпечення для мікропроцесорних систем керування.

Здобуті знання і вміння відображені в результатах навчання

Програмні результати навчання	РН4. Знати принципи роботи технічних засобів автоматизації та вміти обґрунтувати їх вибір на основі аналізу властивостей, призначення і технічних характеристик з урахуванням вимог до системи автоматизації та експлуатаційних умов; демонструвати навички налагодження технічних засобів автоматизації та вбудованих систем керування. РН5. Вміти аналізувати об'єкти автоматизації (за галузями діяльності) і обґрунтовувати вибір структури, алгоритмів та схем керування ними на основі результатів дослідження їх властивостей. РН8. Використовувати сучасні комп'ютерно-інтегровані технології

	для моніторингу та управління технологічними процесами за допомогою засобів людино-машинного інтерфейсу. РН10. Обґрунтовувати вибір структури та розробляти прикладне програмне забезпечення мікропроцесорних систем управління на базі локальних засобів автоматизації та програмованих логічних контролерів для вирішення прикладних проблем у професійній діяльності. РН11. Використовувати телекомунікаційні технології в системах автоматизації.

Теми лекцій:

1. Вступ до технічних засобів захисту автоматизованих систем.
2. Фізичні засоби захисту автоматизованих систем.
3. Мережеві технології та їх захист.
4. Захист програмного забезпечення в автоматизованих системах.
5. Методи резервування та відновлення автоматизованих систем.
6. Системи моніторингу та виявлення загроз.
7. Сучасні тенденції у сфері захисту автоматизованих систем.

Теми практичних занять:

1. Аналіз вразливостей та ризиків в автоматизованих системах.
2. Розробка політики безпеки для захисту автоматизованих систем.

Теми лабораторних занять:

1. Налаштування та тестування засобів контролю доступу.
2. Аналіз трафіку та налаштування мережевих брандмауерів.
3. Дослідження механізмів шифрування та цифрових сертифікатів.
4. Тестування систем виявлення вторгнень (IDS/IPS).
5. Розгортання та налаштування SIEM-систем для моніторингу загроз.
6. Моделювання атак на автоматизовані системи та аналіз їх наслідків.
7. Створення та тестування резервної системи відновлення даних.