

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ІНЖЕНЕРНИЙ ІНСТИТУТ
ЗАПОРІЗЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ФАКУЛЬТЕТ МЕТАЛУРГІЇ
КАФЕДРА АВТОМАТИЗОВАНОГО УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ
ПРОЦЕСАМИ

ЗАТВЕРДЖУЮ



Декан факультету металургії

В.Р. Румянцев
(ініціали та прізвище)

2019 р.

**СИСТЕМИ ЗАХИСТУ У ПРОГРАМНО-ТЕХНІЧНИХ
КОМПЛЕКСАХ АСУ**

(назва навчальної дисципліни)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

підготовки	магістрів
	(назва освітнього ступеня)
спеціальності	151 Автоматизація та комп'ютерно-інтегровані технології
	(шифр, назва спеціальності)
освітньо-професійна програма	Автоматизація та комп'ютерно-інтегровані технології
	(назва)

Укладач Пазюк М.Ю., д.т.н., завідувач кафедри автоматизованого управління технологічними процесами, професор

Обговорено та ухвалено на засіданні кафедри автоматизованого управління технологічними процесами

Протокол № 11 від "17" січня 2020 р.
Завідувач кафедри автоматизованого управління технологічними процесами

М.Ю. Пазюк

Ухвалено науково-методичною радою факультету металургії

Протокол № 5 від "24" січня 2020 р.
Голова науково-методичної ради факультету металургії

Ю.В. Мосейко

2019 рік

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, напрямок підготовки, рівень вищої освіти	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів – 4	Галузь знань 15 Автоматика та управління (шифр і назва)	вільного вибору студента	
Розділів –	Спеціальність 151 Автоматизація та комп'ютерно-інтегровані технології (шифр і назва)	Рік підготовки:	
Загальна кількість годин – 120		3-й	3-й
Тижневих годин для денної форми навчання: аудиторних – 3 самостійної роботи студента – 8	Освітньо-професійна програма Автоматизація та комп'ютерно-інтегровані технології	Лекції	
		22 год.	год.
		Практичні	
			год.
		Лабораторні	
		10 год.	6 год.
		Самостійна робота	
	88 год.	год.	
	Рівень вищої освіти: магістерський	Вид підсумкового контролю: залік	

2. Мета та завдання навчальної дисципліни

Метою вивчення навчальної дисципліни «Системи захисту у програмно-технічних комплексах АСУ» є оволодіння знаннями щодо практичного застосування методів і засобів захисту інформації на прикладі наявних на українському ринку спеціалізованих програмно-апаратних систем.

Основними **завданнями** вивчення дисципліни «Системи захисту у програмно-технічних комплексах АСУ» є: засвоєння методів та прийомів захисту інформації за допомогою конкретних спеціалізованих програмно-апаратних засобів; придбання навичок практичної реалізації захисних механізмів на рівні операційних систем; визначення особливостей реалізації методів захисту в кожній конкретній системі, засвоєння методики застосування цих засобів.

У результаті вивчення навчальної дисципліни студент повинен

знати: види, джерела та носії захищеної інформації; джерела небезпечних сигналів; структуру, класифікацію і основні характеристики технічних каналів витоку інформації;

вміти: працювати із технічними засобами захисту інформації; працювати із захищеними автоматизованими системами; передавати

інформацію по захищеним каналам зв'язку; фіксувати відмови у роботі засобів обчислювальної техніки.

Згідно з вимогами освітньо-професійної програми студенти повинні досягти таких **компетентностей**:

- Здатність використовувати сучасні методи, засоби та технології дослідження та розробки об'єктів професійної діяльності;
- Здатність використовувати довідкову літературу та професійні знання та практичні навички в галузі автоматизації для дослідження та визначення технічного та програмного забезпечення систем керування;
- Здатність до аналізу схемних рішень електронних пристроїв, та їх функцій;
- Здатність налагоджувати та обслуговувати програмно-технічні засоби систем керування, визначати ефективні та раціональні шляхи управління персоналом;
- Здатність оцінювати ефективність структурно-алгоритмічних та програмно-технічних рішень в складі систем керування;
- Здатність аналізувати вплив роботи системи автоматичного управління на показники якості виробничого (технологічного) процесу.

Програма навчальної дисципліни

Розділ 1. Технічні методи та засоби, технології захисту інформації

Тема 1. Поняття захисту інформації

Зміст. Поняття інформації, захисту інформації, інформаційної системи, безпеки автоматизованих систем обробки інформації. Цілі захисту інформації. Базові властивості інформації.

Тема 2. Санкціонований та несанкціонований доступ

Зміст. Аналогова модель екстраполятора. Імпульсна модель дискретного сигналу.

Тема 3. Поняття загрози, вразливості, ризику

Зміст. Поняття загрози, класифікація загроз. Поняття вразливості, атаки на систему. Поняття ризику. Задачі спеціаліста з інформаційної безпеки.

Тема 4. Канали реалізації загроз

Зміст. Види витоку інформації. Поняття каналу витоку інформації, основні канали витоку інформації. Класифікація зловмисників.

Тема 5. Основні принципи забезпечення інформаційної безпеки

Зміст. Принципи системності, комплексності, безперервності захисту, гнучкості управління та застосування захисних механізмів.

Тема 6. Заходи забезпечення безпеки комп'ютерних систем

Зміст. Правові, морально-етичні, організаційно-адміністративні, фізичні, апаратно-програмні заходи забезпечення безпеки комп'ютерних систем.

Розділ 2. Захист інформації у обчислювальних мережах

Тема 7. Атаки на мережеві служби

Зміст. Класифікація атак за основними механізмами реалізації загроз. Мережеві сканери

Тема 8. Адаптивна безпека у обчислювальних мережах. Мережеві екрани

Зміст. Поняття адаптивної безпеки та системи виявлення атак. Класифікація мережевих екранів

Тема 9. Віддалений доступ до мережі

Зміст. Протоколи доступу. Тунелювання. Цифрові сертифікати.

Тема 10. Політика безпеки

Зміст. Поняття політики інформаційної безпеки. Основні вимоги до політики безпеки. Етапи її розробки.

Розділ 3. Захист інформації у системах управління базами даних

Тема 11. Політика безпеки

Зміст. Загрози безпеки базам даних: загальні та специфічні. Вимоги безпеки д баз даних.

Тема 12. Критерії захищеності баз даних

Зміст. Критерії захищеності комп'ютерних мереж. Критерії оцінювання надійних комп'ютерних мереж. Моделі безпеки у системах управління базами даних. механізми забезпечення цілісності баз даних.

Теми лабораторних занять

№ теми з/прогр	Назва теми	Кількість годин	
		д.ф.	з.ф.
	Засоби захисту доступу до комп'ютеру		
	Канали витоку інформації. Захист приміщень		
	Ефективність інформаційної безпеки		
	Побудова системи інформаційної безпеки		
	Мережеві атаки		
Разом			