ПАСПОРТ СПЕЦІАЛЬНОСТІ
05.13.21 - системи захисту інформації

І. Формула спеціальності:

Дослідження теоретичних, науково-технічних і технологічних проблем, пов'язаних із організацією, створенням методів та засобів забезпечення захисту інформації при її зберіганні, обробці й передачі з використанням сучасних математичних методів, інформаційних технологій та технічних засобів.

ІІ. Напрямки досліджень:

- Теоретичні, методологічні, технічні, технологічні й організаційні основи створення комплексних систем захисту інформації (СЗІ), зокрема інформації, що зберігається, оброблюється і передається в комп'ютерних системах і мережах.
- Організація, архітектура, методологія проектування, технологія функціонування СЗІ.
- Шифри, шифросистеми, криптографічні протоколи та способи вибору систем криптозахисту, адекватних прийнятій політиці безпеки інформації.
- Методологія криптографічного аналізу та побудови оцінок криптографічної стійкості шифросистем, методи викриття механізмів криптоперетворень, зокрема дешифрування.
- Математичні моделі інформаційних структур, що потребують захисту, шифрів, шифросистем та криптографічних протоколів.
- Математичні й обчислювальні методи розрахунку надійності криптосистем, прогнозування оцінок криптографічної стійкості, розв'язання завдань криптографічного аналізу та синтезу шифросистем і криптографічних протоколів.
- Технічні канали відпливу інформації та їх моделі, нові технології й засоби захисту інформації від відпливу технічними каналами. Норми ефективного захисту інформації від відпливу технічними каналами.
- Моделювання процесів нападу на інформацію та її захисту.
- Методи і засоби вимірювання й обчислення параметрів небезпечних сигналів.

ІІІ. Галузі наук, з яких присуджуються наукові ступені.

Технічні науки