Силабус

«ДВА.3.01.17 Математичні основи захисту інформації»
Спеціальність 126 «Інформаційні системи та технології»
ОНП «Інформаційні системи та технології»

Ступінь вищої освіти	Доктор філософії
Дисципліна	Дисципліни вільного вибору аспіранта
Рік	2
Кредити	4 кредити ЄКТС
Мова	Українська
Вид занять	Лекції, практичні заняття, консультації, самостійна робота
Методи навчання	Навчальна бесіда, складання схем і порівняльних таблиць
Форми навчання	Денна
Вид контролю	Екзамен
Вивчається	Забезпечує професійний розвиток, спрямований на формування концептуальних та методологічних знань у галузі математичних основ захисту інформації. Розглядаються математичні закони криптології та криптоаналізу. Захист інформації розглядається як сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру. В рамках дисципліни вивчаються основні математичні елементи формування: • Криптосистем • Шифрограм • Алгоритми шифрування • Псевдовипадкові послідовності • Паралельні обчислення
Навчальна логістика / зміст курсу	1. Історія криптографії. 2. Сучасна криптографія. 3. Симетричне шифрування. 4. Асиметричне шифрування. 5. Шифрування та розшифрування. 6. Стійка криптографія. 7. Дія криптографії. 8. Симетричне шифрування та керування ключами. 9. Ключі. 10. Цифровий підпис. 11. Хеш-функція. 12. Цифровий сертифікат. 13. Ключова фраза. 14. Поділ ключа. 15. Стандартизація у криптографії.