Код та назва дисципліни	2у-09-34_Криптографія та криптоаналіз
Рекомендується для галузі знань *(спеціальності, освітньої програми)*	01 Освіта / Педагогіка, 10 Природничі науки, 12 Інформаційні технології, 15 Автоматизація та приладобудування, 17 Електроніка та телекомунікації.
Кафедра	Теоретичної фізики.
П.І.П. НПП *(за можливості)*	Турінов Андрій Миколайович.
Рівень ВО	Другий (магістерський) рівень.
Курс, семестр *(в якому буде викладатись)*	Перший курс, 1 або 2 семестр.
Мова викладання	Українська.
Пререквізити (передумови вивчення дисципліни)	Ефективність засвоєння змісту дисципліни значно підвищиться, якщо студент попередньо опанував матеріал таких дисциплін: математичний аналіз, алгебра та геометрія; теорія ймовірностей та основи програмування.
Що буде вивчатися	Методи і засоби семантичного перетворення інформації з метою забезпечення секретності її зберігання, історія розвитку криптографії, останні досягненнями в цій галузі, теоретична і практична значимість криптографічних систем та криптографічних протоколів.
Чому це цікаво/треба вивчати	Знання, вміння і навики, придбані при вивченні дисципліни необхідні як при теоретичних дослідженнях у галузі криптографічної інформації, так і при практичної діяльності при побудові, експертизі та застосуванні сучасних систем захисту інформації із криптографічною підсистемою.
Чого можна навчитися *(результати навчання)*	Базовим принципам інформаційної безпеки комп'ютерних мереж; організаційним заходам і планування безпеки інформації.; криптографічним методи і засобам захисту інформації; шифруванню великих повідомлень і потоків даних; алгоритмам формування довгих електронних та коротких цифрових підписів; системам технічного захисту інформаційних об'єктів.
Як можна користуватися набутими знаннями і уміннями *(компетентності)*	Програмно реалізовувати алгоритми шифрування та дешифрування інформації; робити оцінку обчислювальної похибки; визначати стійкість використаного методу відносно взламування та надійність системи; практично використовувати симетричні та асиметричні алгоритми захисту; знати сучасні підходи до зламування криптосистеми; використовувати потокове шифрування.
Інформаційне забезпечення	Бібліотека ДНУ, методичні розробки кафедри теоретичної фізики та факультету ФЕКС.
Види навчальних занять *(лекції, практичні, семінарські, лабораторні заняття тощо)*	Лекції – 48 годин.
Вид семестрового контролю	диференційований залік
Максимальна кількість здобувачів	40
Мінімальна кількість здобувачів *(тільки для мовних та творчих дисциплін)*	