МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ  
 ім. Семена КУЗНЕЦЯ

Кафедра кібербезпеки та інформаційних технологій

Екзаменаційний білет

з дисципліни

“Теоретичні основи кібербезпеки”

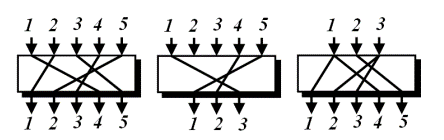
Білет №7

1. Як класифікуються алгоритми шифрування?

2. Поясніть сутність адитивного шифру підстановки.

3. Назвіть переваги та недоліки ЕЦП RSA

4. Здійсніть перестановку бітів для прямого P-блоку, показаного на рис.



якщо на його вході діє послідовність: (10110)2.

Екзаменатор

Професор кафедри кібербезпеки

та інформаційних технологій,

д.т.н., с.н.с. А. Чугай

Зав. кафедри кафедри кібербезпеки

та інформаційних технологій,

д.т.н., проф. О. Старкова

Затверджено на заіданні кафедри кібербезпеки та

інформаційних технологій протокол №