

---

**Криптологія та захист інформації в автоматизованих системах**

**Білет №1**

1. Загальні поняття інформаційної безпеки та захисту інформації
  2. Методи та види НСД. Засоби захисту від НСД
  3. Симетричні алгоритми криптоаналізу. Диференційний і лінійний криптоаналіз
- 

**Криптологія та захист інформації в автоматизованих системах**

**Білет №2**

1. Державна політика забезпечення інформаційної безпеки
  2. Ідентифікація й автентифікація. Основні поняття
  3. Загрози безпеці операційних систем
- 

**Криптологія та захист інформації в автоматизованих системах**

**Білет №3**

1. Основні підходи до забезпечення інформаційної безпеки, їх переваги та недоліки
  2. Парольна автентифікація. Одноразові паролі
  3. Побудова захищених операційних систем
- 

**Криптологія та захист інформації в автоматизованих системах**

**Білет №4**

1. Основні визначення й критерії класифікації загроз
  2. Технології ідентифікації й автентифікації
  3. Принципи створення захищених операційних систем
- 

**Криптологія та захист інформації в автоматизованих системах**

**Білет №5**

1. Найпоширеніші загрози доступності
  2. Автентифікація по багаторазових паролях. Система Kerberos
  3. Адміністративні заходи захисту операційних систем
- 

**Криптологія та захист інформації в автоматизованих системах**

**Білет №6**

1. Основні загрози цілісності
  2. Протоколи автентифікації для віддаленого доступу
  3. Політика безпеки операційних систем
- 
-

---

**Криптологія та захист інформації в автоматизованих системах**

**Білет №7**

1. Основні загрози конфіденційності
  2. Керування доступом. Основні поняття
  3. Архітектура комплексу засобів захисту операційних систем
- 

**Криптологія та захист інформації в автоматизованих системах**

**Білет №8**

1. Шкідливе програмне забезпечення
  2. Рольове керування доступом
  3. Розмежування доступу, ідентифікація, автентифікація й авторизація в операційних системах
- 

**Криптологія та захист інформації в автоматизованих системах**

**Білет №9**

1. Особливості сучасних автоматизованих систем, істотні з погляду безпеки
  2. Керування доступом у Java-середовищі
  3. Підсистема аудита в операційних системах
- 

**Криптологія та захист інформації в автоматизованих системах**

**Білет №10**

1. Організаційне забезпечення інформаційної безпеки на підприємстві. Служби безпеки.
  2. Моніторинг систем інформаційної безпеки
  3. Захист машинних носіїв інформації
- 

**Криптологія та захист інформації в автоматизованих системах**

**Білет №11**

1. Основні задачі служби інформаційної безпеки підприємства
  2. Протоколювання й аудит. Основні поняття та етапи
  3. Основні положення захисту інформації, збереженої на жорстких дисках
- 

**Криптологія та захист інформації в автоматизованих системах**

**Білет №12**

1. Основні поняття організаційно-технічного рівня інформаційної безпеки
  2. Активний аудит. Функціональні компоненти й архітектура
  3. Способи знищення інформації, збереженої на жорстких дисках
-

---

**Криптологія та захист інформації в автоматизованих системах**

**Білет №13**

1. Технічні канали витоку інформації. Рекомендації із захисту
  2. Основні поняття та визначення криптології
  3. Антивірусне ПЗ. Методи знаходження вірусів
- 

**Криптологія та захист інформації в автоматизованих системах**

**Білет №14**

1. Охоронні системи
  2. Шифрування. Вимоги та стандарти
  3. Екранування. Основні поняття. Архітектурні аспекти
- 

**Криптологія та захист інформації в автоматизованих системах**

**Білет №15**

1. Законодавчий рівень інформаційної безпеки, його важливість
  2. Симетричні алгоритми шифрування. Стандарти
  3. Класифікація міжмережних екранів
- 

**Криптологія та захист інформації в автоматизованих системах**

**Білет №16**

1. Українське законодавство в сфері інформаційної безпеки
  2. Шифр Цезаря. Шифр Віженера. Шифр Вернама
  3. Тунелювання
- 

**Криптологія та захист інформації в автоматизованих системах**

**Білет №17**

1. Оцінні стандарти й технічні специфікації. "Оранжева книга" як оцінний стандарт
  2. Алгоритм шифрування DES та AES. Загальна схема
  3. Політика безпеки при роботі в Інтернеті
- 

**Криптологія та захист інформації в автоматизованих системах**

**Білет №18**

1. Інформаційна безпека розподілених систем. Рекомендації X.800. Механізми безпеки. Класи безпеки
  2. Асиметричні алгоритми шифрування. Приклади асиметричних криптосистем
  3. Аналіз захищеності
-

---

**Криптологія та захист інформації в автоматизованих системах**

**Білет №19**

1. Мережні сервіси безпеки. Мережні механізми безпеки. Інтерпретація "Оранжевої книги" для мережних конфігурацій
  2. Криптосистема з відкритим ключем. Загальна схема шифрування
  3. Доступність. Основи заходів забезпечення високої доступності
- 

**Криптологія та захист інформації в автоматизованих системах**

**Білет №20**

1. Гармонізовані критерії Європейських країн
  2. Однобічні функції та функції „з секретом”
  3. Відмовостійкість і зона ризику. Забезпечення відмовостійкості
- 

**Криптологія та захист інформації в автоматизованих системах**

**Білет №21**

1. Адміністративний рівень інформаційної безпеки. Політика безпеки
  2. Алгоритми шифрування RSA та Ельгамала
  3. Програмне забезпечення проміжного шару
- 

**Криптологія та захист інформації в автоматизованих системах**

**Білет №22**

1. Види політики безпеки
  2. Відкриті засоби шифрування
  3. Забезпечення обслуговуваності
- 

**Криптологія та захист інформації в автоматизованих системах**

**Білет №23**

1. Математичні моделі безпеки
  2. Контроль цілісності. Цифрові сертифікати
  3. Менеджмент інформаційної безпеки. Можливості типових систем менеджменту
- 

**Криптологія та захист інформації в автоматизованих системах**

**Білет №24**

1. Програма безпеки
  2. Функція хешування. Її властивості
  3. Організаційні принципи побудови СЗІ в захищених АС
-

---

**Криптологія та захист інформації в автоматизованих системах**  
**Білет №25**

1. Керування ризиками
  2. Електронний цифровий підпис. Класична схема
  3. Методи побудови СЗІ в захищених АС
- 

**Криптологія та захист інформації в автоматизованих системах**  
**Білет №26**

1. Основні класи заходів процедурного рівня. Керування персоналом
  2. Інфраструктура ЕЦП та ЕДО
  3. Передпроектні аспекти створення СЗІ та захищених АС
- 

**Криптологія та захист інформації в автоматизованих системах**  
**Білет №27**

1. Підтримка працездатності.
  2. Основні підходи до визначення стійкості криптосистем і криптографічних протоколів
  3. Забезпечення інформаційної безпеки на подальших стадіях побудови захищених АС
- 

**Криптологія та захист інформації в автоматизованих системах**  
**Білет №28**

1. Реагування на порушення режиму безпеки. Планування відбудовних робіт
  2. Методи криптоаналізу
  3. Аналіз захищеності інформації в АС
- 

**Криптологія та захист інформації в автоматизованих системах**  
**Білет №29**

1. Три основні категорії інформаційної безпеки. Їх визначення
  2. Визначення понять, пов'язаних з НСД
  3. Загальноприйняті вимоги до сучасних криптографічних систем захисту інформації
- 

**Криптологія та захист інформації в автоматизованих системах**  
**Білет №30**

1. Основні властивості інформації у сенсі інформаційної безпеки
  2. Ідентифікація за допомогою біометричних даних
  3. Симетричні алгоритми шифрування. Схематичне та математичне представлення
-