

Министерство образования Республики Беларусь  
Учреждение образования  
Белорусский государственный университет информатики и  
Радиоэлектроники

Факультет информационных технологий и управления  
Кафедра интеллектуальных информационных технологий

Отчет по лабораторной работе №3  
по курсу “Средства и методы защиты информации в интеллектуальных  
системах”

Выполнил:  
Студент гр. 321703

Титов А.В.

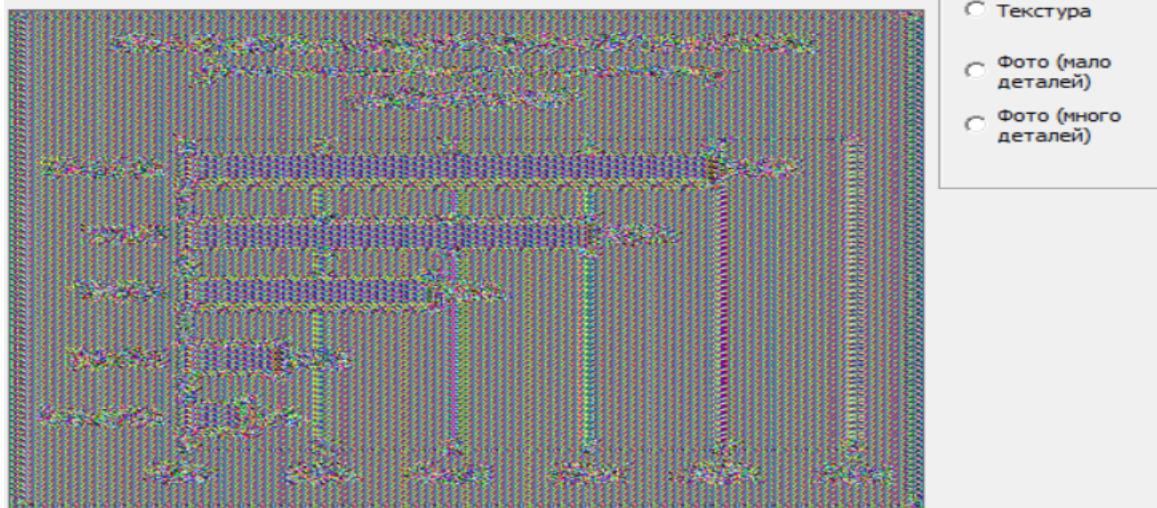
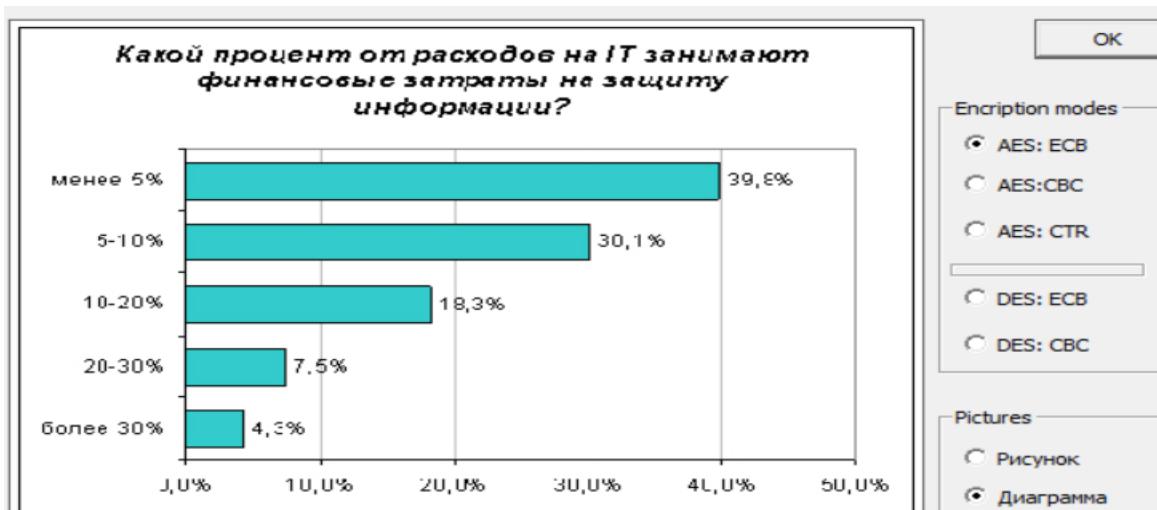
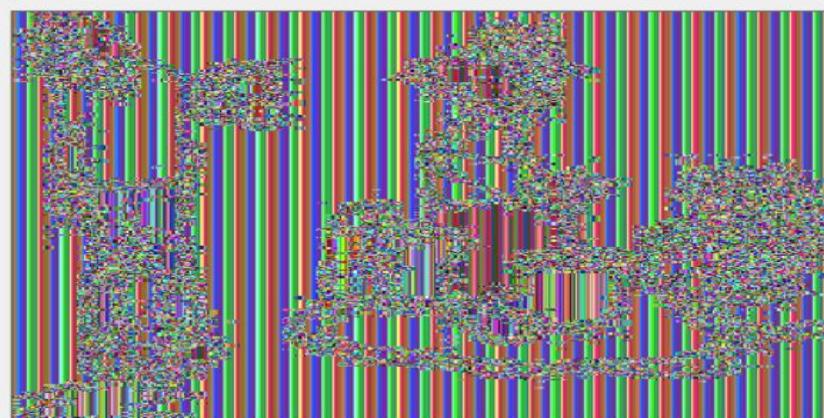
Проверил: Сальников Д.А.

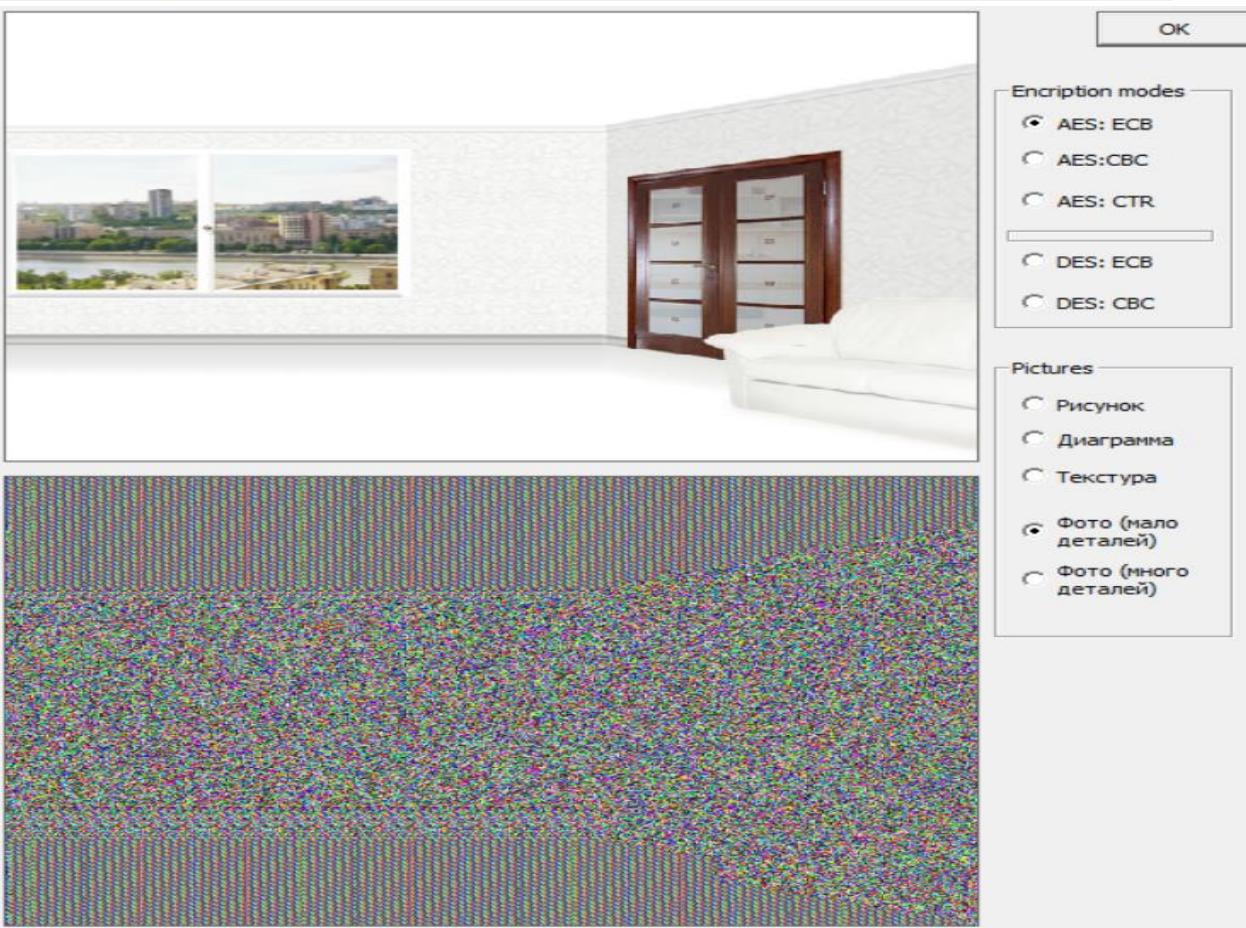
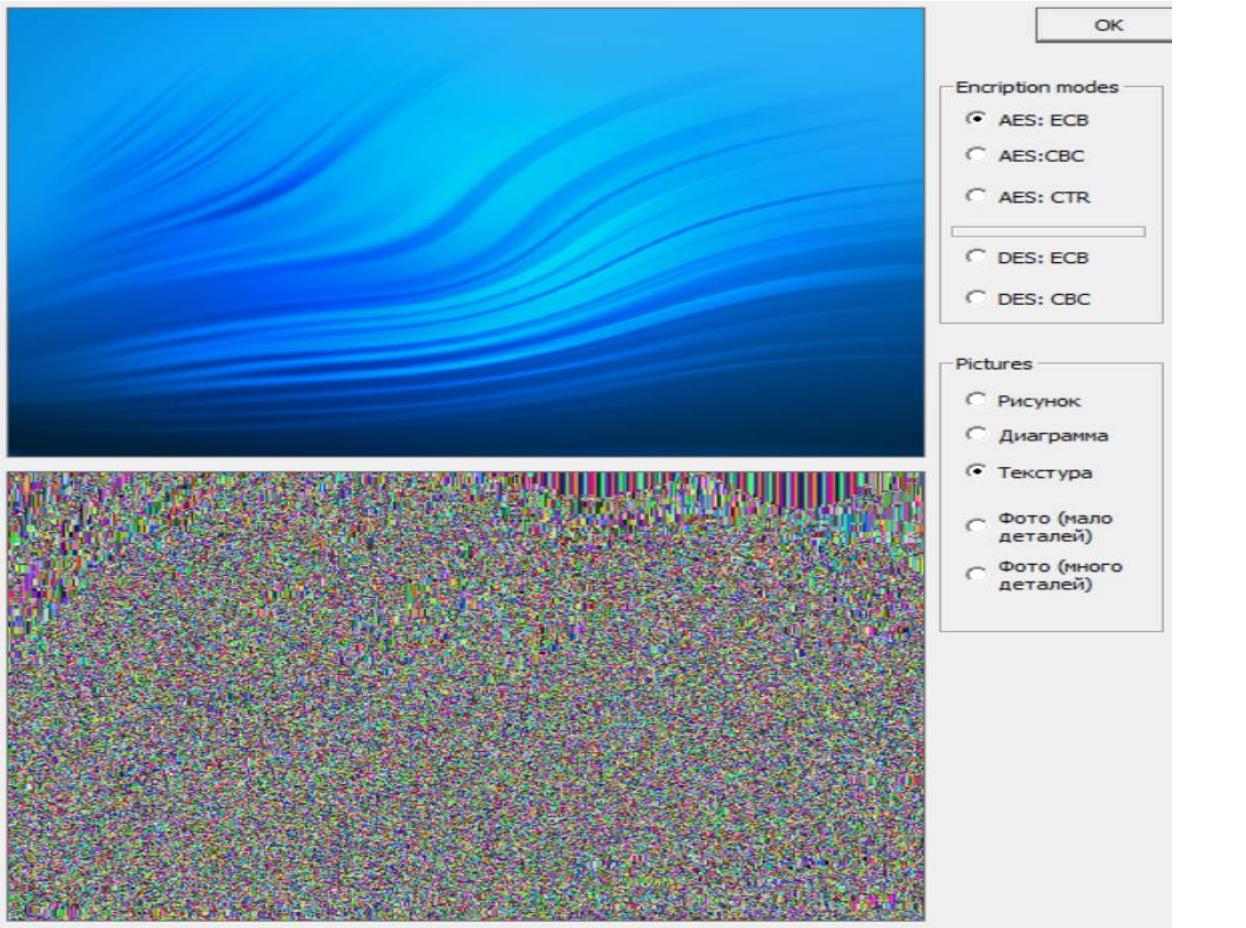
Минск 2025

## **ЛАБОРАТОРНАЯ РАБОТА № 3 “РЕЖИМЫ ПРИМЕНЕНИЯ БЛОЧНЫХ ШИФРОВ”**

### **Цель:**

- 1) Зашифровать предложенные изображения всеми возможными алгоритмами во всех возможных режимах. Результаты шифрования отразить в отчете в виде скриншотов.
- 2) Оценить полученные результаты и объяснить их причины.
- 3) Дать рекомендации по применению алгоритмов шифрования и их режимов в зависимости от типов изображения, шифрования и особенностей применения.
- 4) Дать ответ на вопрос: как влияет размер блока шифра на результат шифрования и почему?







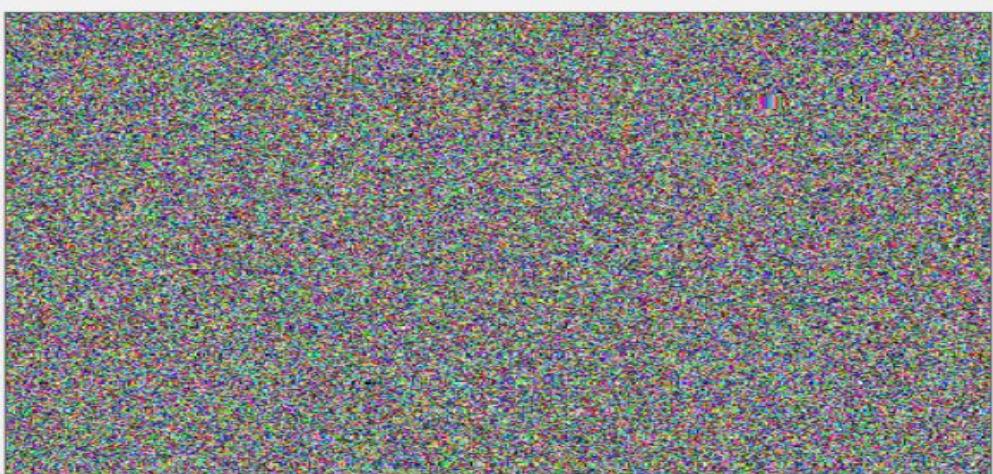
OK

Encryption modes

- AES: ECB
- AES:CBC
- AES: CTR
- 
- DES: ECB
- DES: CBC

Pictures

- Рисунок
- Диаграмма
- Текстура
- 
- Фото (мало деталей)
- Фото (много деталей)



OK

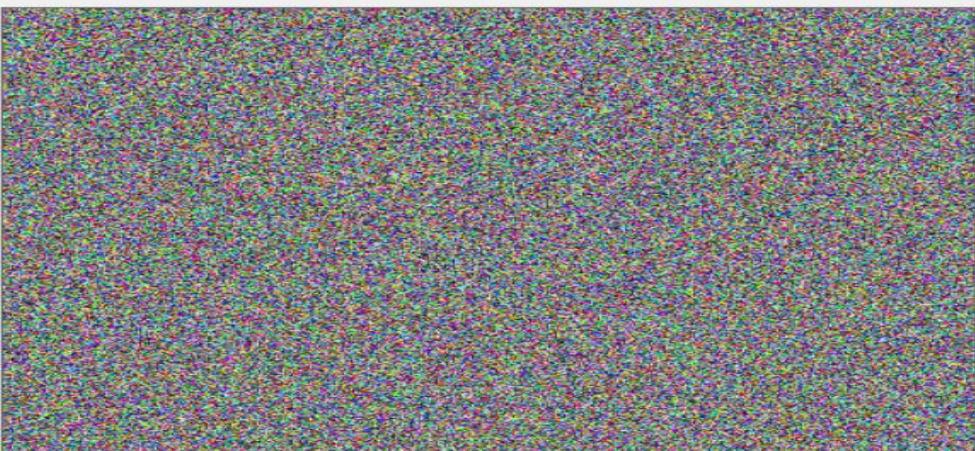
Encryption modes

- AES: ECB
- AES:CBC
- AES: CTR
- 
- DES: ECB
- DES: CBC

Pictures

- Рисунок
- Диаграмма
- Текстура
- 
- Фото (мало деталей)
- Фото (много деталей)





OK

Encription modes

- AES: ECB
- AES:CBC
- AES: CTR
- DES: ECB
- DES: CBC

Pictures

- Рисунок
- Диаграмма
- Текстура
- Фото (мало деталей)
- Фото (много деталей)

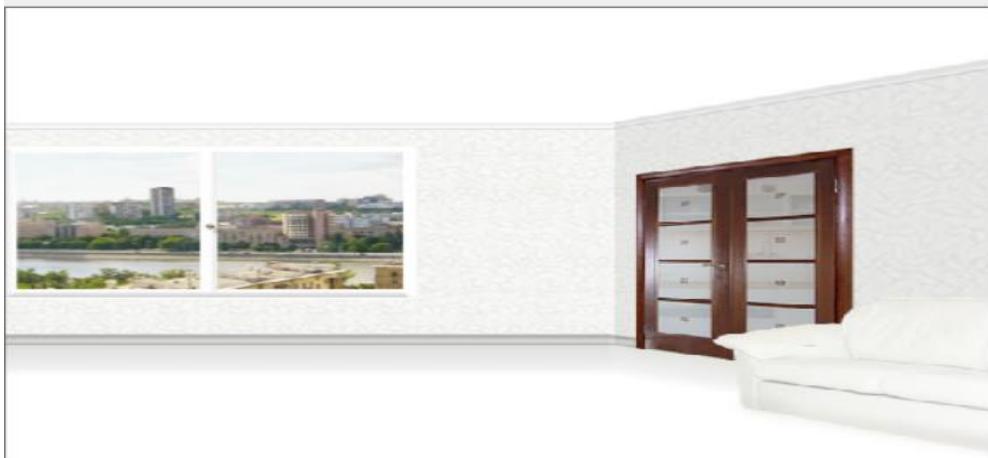
OK

Encription modes

- AES: ECB
- AES:CBC
- AES: CTR
- DES: ECB
- DES: CBC

Pictures

- Рисунок
- Диаграмма
- Текстура
- Фото (мало деталей)
- Фото (много деталей)



OK

Encryption modes

- AES: ECB
  - AES:CBC
  - AES: CTR
- 
- DES: ECB
  - DES: CBC

Pictures

- Рисунок
- Диаграмма
- Текстура
- Фото (мало деталей)
- Фото (много деталей)



OK

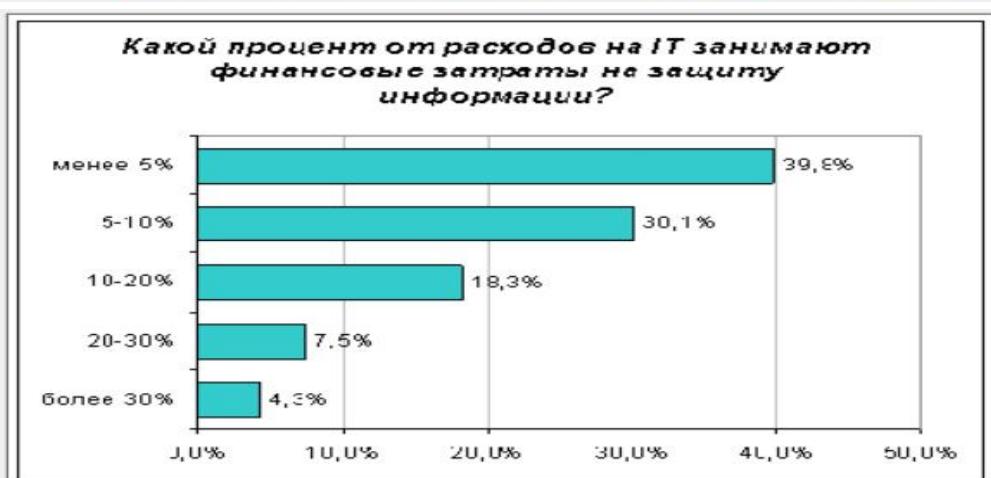
Encryption modes

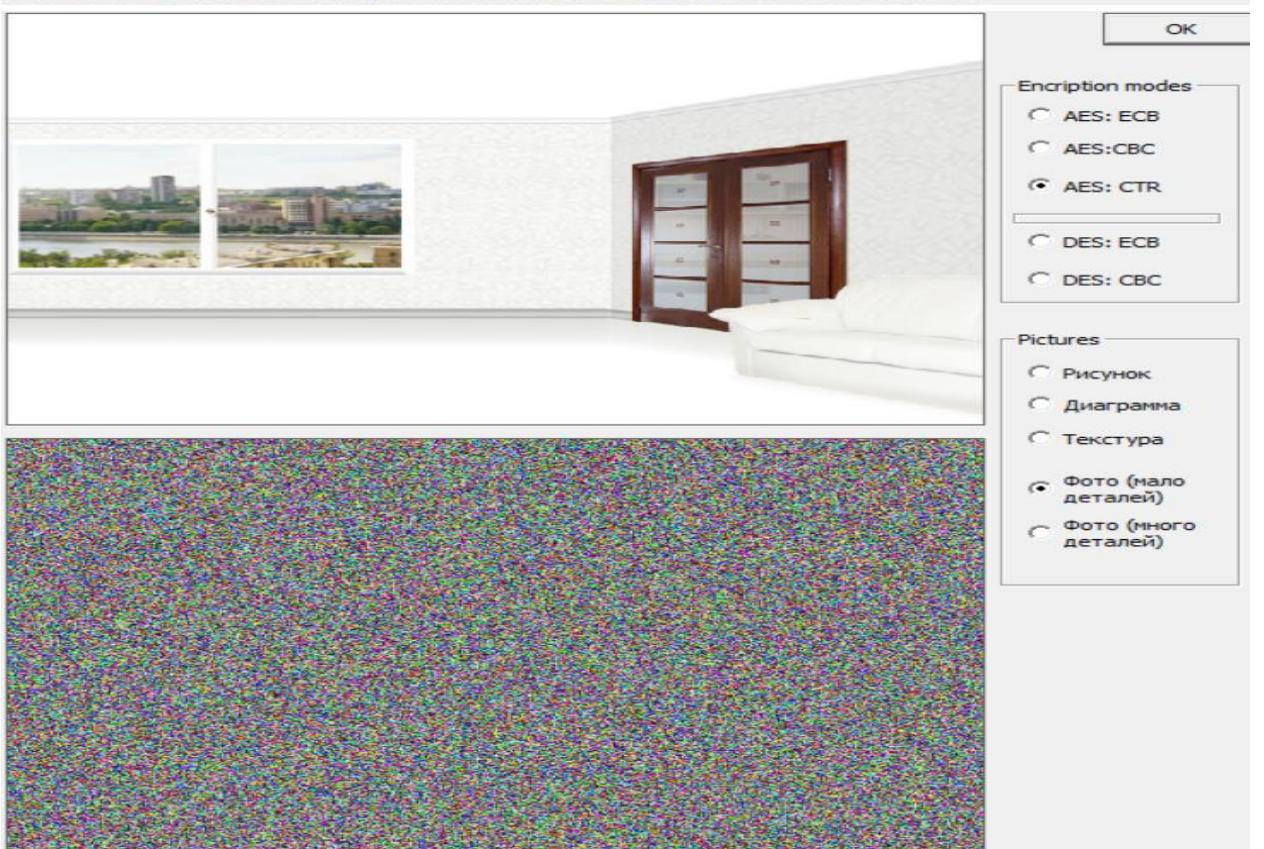
- AES: ECB
  - AES:CBC
  - AES: CTR
- 
- DES: ECB
  - DES: CBC

Pictures

- Рисунок
- Диаграмма
- Текстура
- Фото (мало деталей)
- Фото (много деталей)









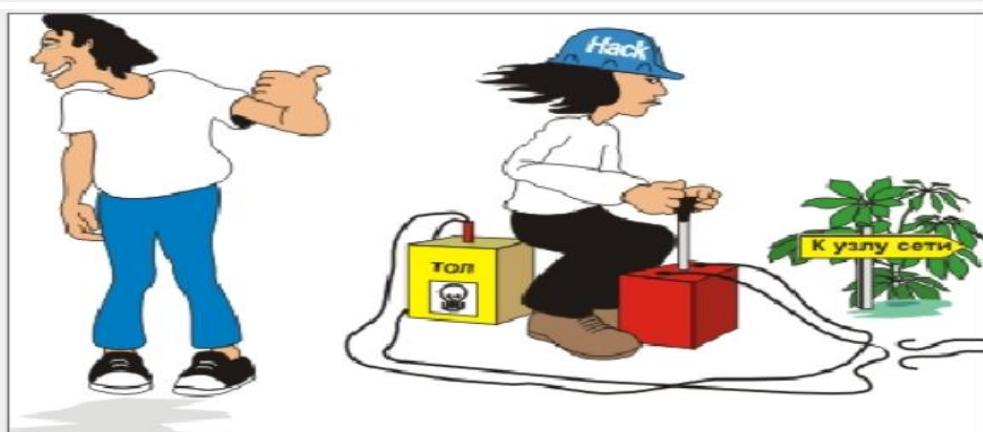
OK

Encryption modes

- AES: ECB
- AES:CBC
- AES: CTR
- DES: ECB
- DES: CBC

Pictures

- Рисунок
- Диаграмма
- Текстура
- Фото (мало деталей)
- Фото (много деталей)



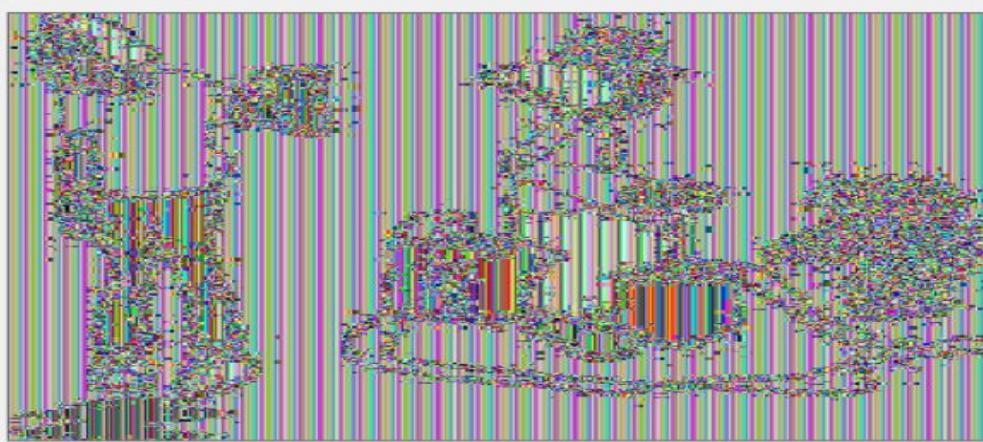
OK

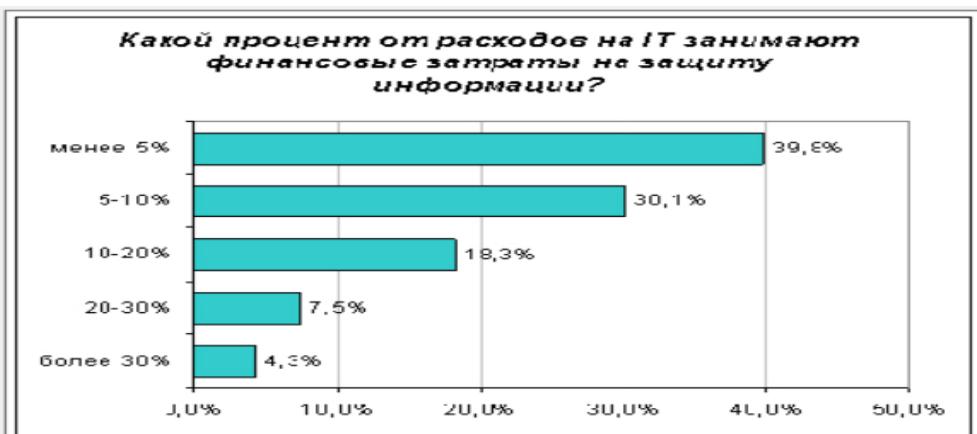
Encryption modes

- AES: ECB
- AES:CBC
- AES: CTR
- DES: ECB
- DES: CBC

Pictures

- Рисунок
- Диаграмма
- Текстура
- Фото (мало деталей)
- Фото (много деталей)





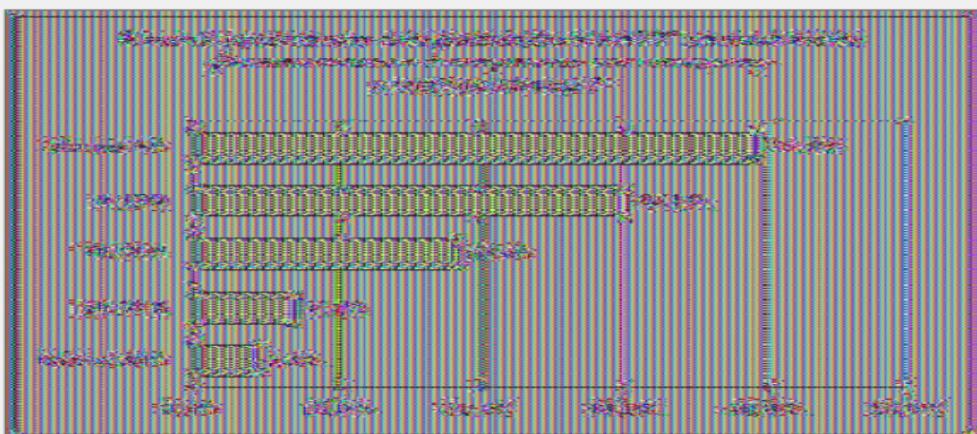
OK

## Encryption modes

- AES: ECB
- AES:CBC
- AES: CTR
- DES: ECB
- DES: CBC

## Pictures

- Рисунок
- Диаграмма
- Текстура
- Фото (мало деталей)
- Фото (много деталей)



OK



## Encryption modes

- AES: ECB
- AES:CBC
- AES: CTR
- DES: ECB
- DES: CBC

## Pictures

- Рисунок
- Диаграмма
- Текстура
- Фото (мало деталей)
- Фото (много деталей)



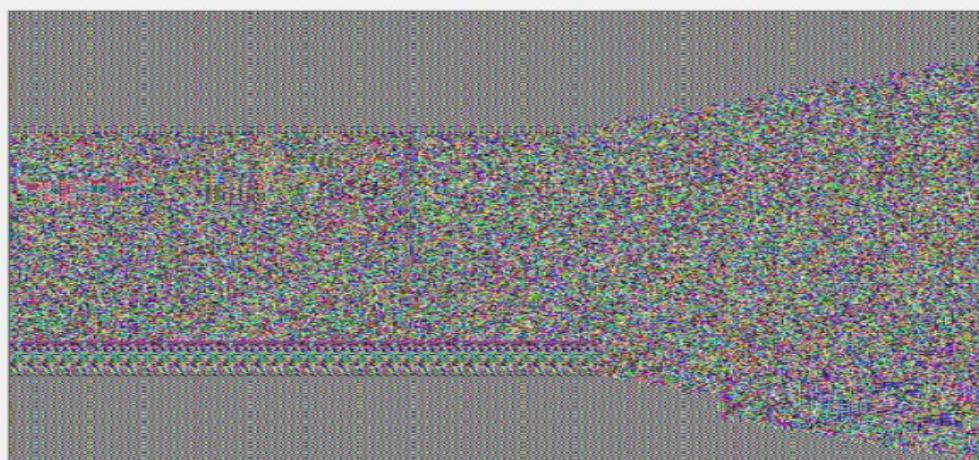
OK

Encryption modes

- AES: ECB
- AES:CBC
- AES: CTR
- DES: ECB
- DES: CBC

Pictures

- Рисунок
- Диаграмма
- Текстура
- Фото (мало деталей)
- Фото (много деталей)



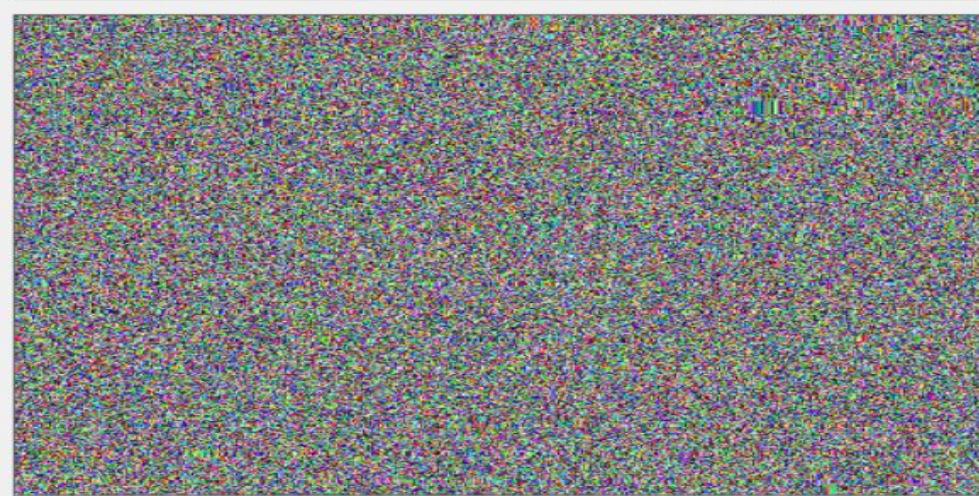
OK

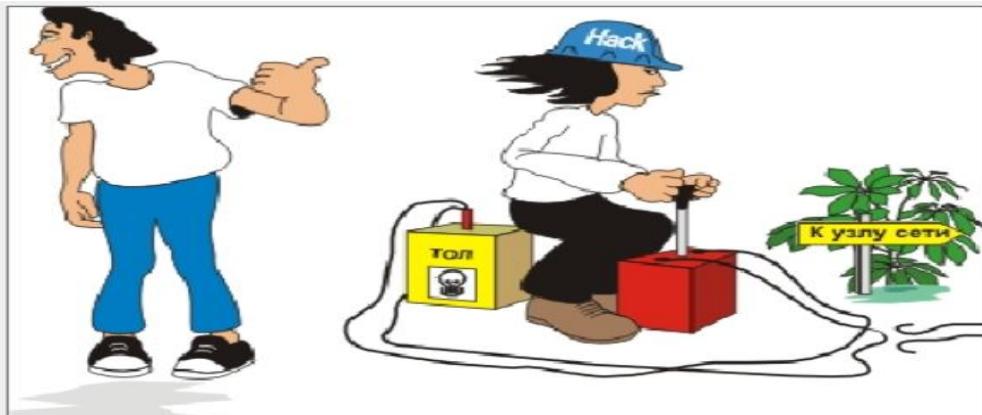
Encryption modes

- AES: ECB
- AES:CBC
- AES: CTR
- DES: ECB
- DES: CBC

Pictures

- Рисунок
- Диаграмма
- Текстура
- Фото (мало деталей)
- Фото (много деталей)





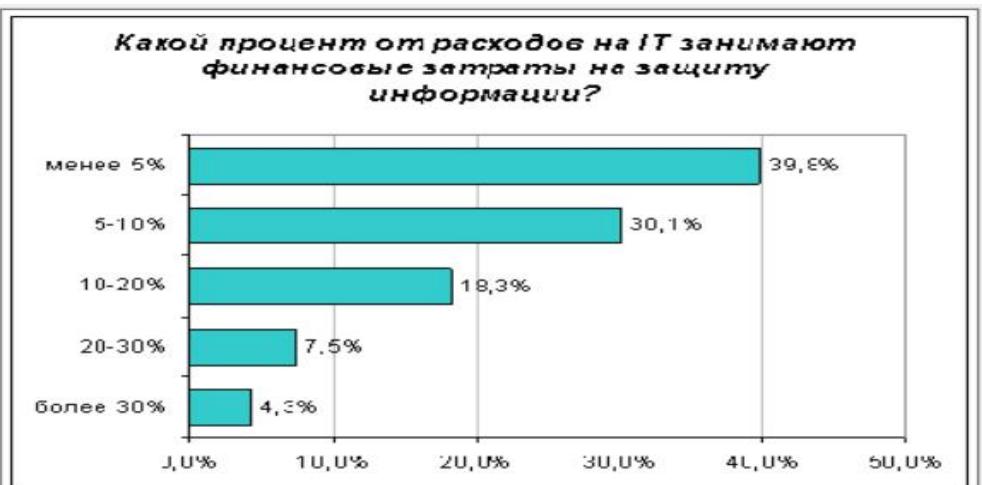
OK

## Encription modes

- AES: ECB
  - AES:CBC
  - AES: CTR
- 
- DES: ECB
  - DES: CBC

## Pictures

- Рисунок
  - Диаграмма
  - Текстура
- 
- Фото (мало деталей)
  - Фото (много деталей)



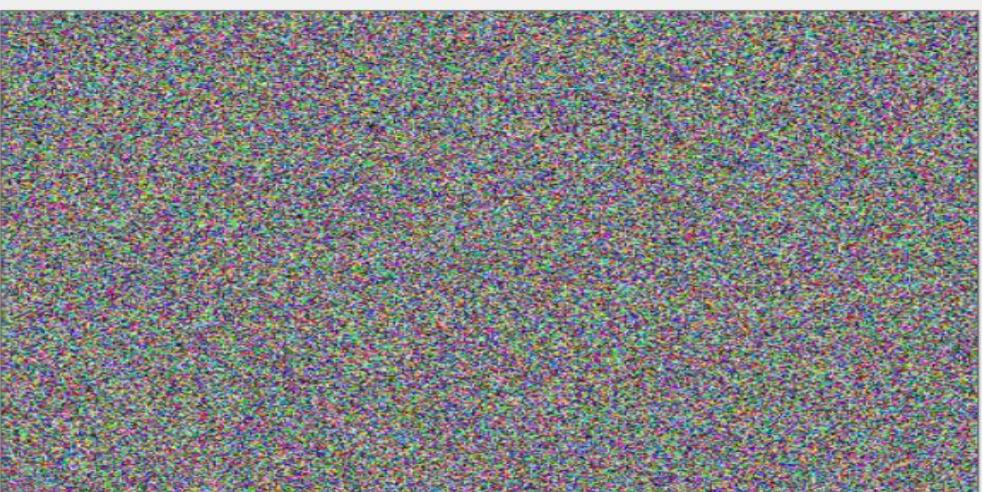
OK

## Encription modes

- AES: ECB
  - AES:CBC
  - AES: CTR
- 
- DES: ECB
  - DES: CBC

## Pictures

- Рисунок
  - Диаграмма
  - Текстура
- 
- Фото (мало деталей)
  - Фото (много деталей)



OK

Encryption modes

- AES: ECB
- AES:CBC
- AES: CTR
- DES: ECB
- DES: CBC

Pictures

- Рисунок
- Диаграмма
- Текстура
- Фото (мало деталей)
- Фото (много деталей)



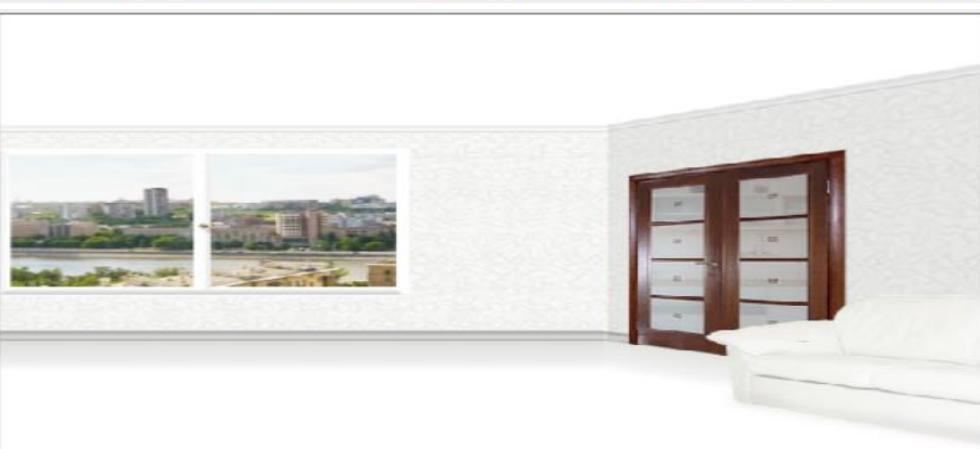
OK

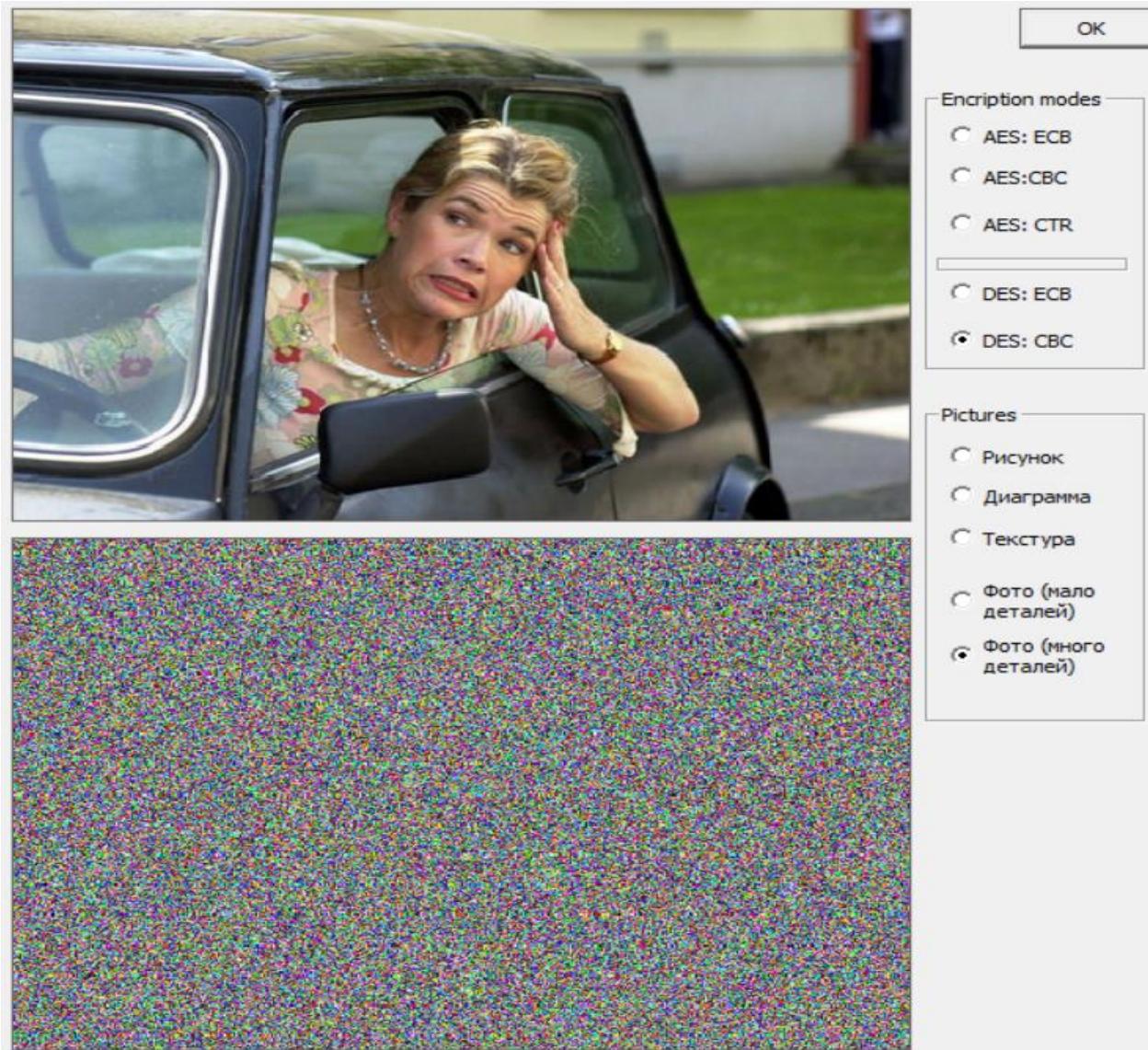
Encryption modes

- AES: ECB
- AES:CBC
- AES: CTR
- DES: ECB
- DES: CBC

Pictures

- Рисунок
- Диаграмма
- Текстура
- Фото (мало деталей)
- Фото (много деталей)





## 2. Оценка полученных результатов и объяснение их причин

### Режим ECB (Electronic Codebook - Электронная кодовая книга)

- **Результат:** На зашифрованном изображении **четко видны контуры** исходного изображения. Текстуры, градиенты и большие области одного цвета превращаются в узнаваемые узоры.
- **Причина:** Это главный недостаток ECB. **Однаковые блоки открытого текста шифруются в одинаковые блоки шифртекста.** Поскольку в изображениях (особенно в компьютерной графике и диаграммах) часто встречаются большие области с одинаковыми пикселями (например, белый фон, синее небо), эти области после шифрования превратятся в однородные "узоры". Шифр не скрывает статистические свойства данных.

## **Режим CBC (Cipher-Block Chaining - Сцепление блоков шифротекста)**

- **Результат:** Зашифрованное изображение представляет собой **абсолютно случайный шум**. Никаких контуров или узнаваемых деталей видно не будет.
- **Причина:** Каждый блок открытого текста перед шифрованием **комбинируется с предыдущим блоком шифртекста (XOR)**. Это означает, что даже если два блока открытого текста одинаковы, они будут зашифрованы в совершенно разные блоки шифртекста. Эффект распространения ошибки и зависимость от всех предыдущих данных полностью устраняют видимые паттерны.

## **Режим CTR (Counter - Счетчик)**

- **Результат:** Аналогично CBC, результат выглядит как **случайный шум** без каких-либо видимых закономерностей.
- **Причина:** Этот режим превращает блочный шифр в поточный. Шифруется не сам данные, а значение счетчика. Затем результат XORится с открытым текстом. **Одинаковые блоки открытого текста будут зашифрованы по-разному**, потому что значение счетчика всегда уникально для каждого блока. Это также исключает появление паттернов.

## **Сравнение AES и DES:**

- Визуально, в рамках одного режима (CBC или CTR), **разница между AES и DES будет не видна**. Оба дадут на выходе случайный шум.
- Разница заключается в **криптографической стойкости**. DES (64-битный, с ключом 56 бит) считается устаревшим и может быть взломан полным перебором (brute-force) за разумное время на современном оборудовании. AES (128-битный блок, ключи 128/192/256 бит) является современным и надежным стандартом.

## **3. Рекомендации**

### **Выбор алгоритма:**

1. **AES:** Является **безальтернативным выбором** для любых новых приложений. Соответствует современным стандартам безопасности.
2. **DES: НЕ СЛЕДУЕТ ИСПОЛЬЗОВАТЬ** для защиты новых данных. Его применение оправдано только для обеспечения обратной совместимости со старыми системами.

## Выбор режима:

### 1. ECB:

- **Не подходит** для шифрования любых данных с избыточностью (изображения, видео, документы).
- **Может быть применим** только для шифрования случайных данных или данных, которые сами по себе не несут видимых паттернов (например, уже предварительно зашифрованные данные). Но даже в этом случае предпочтительнее другие режимы.

### 2. CBC:

- **Хороший выбор** для шифрования файлов и данных, передаваемых по каналу с установленным соединением.
- **Недостаток:** Шифрование последовательное (не может быть распараллелено), так как каждый блок зависит от предыдущего. Также требует механизма передачи уникального IV (вектор инициализации) для каждого шифрования.

### 3. CTR:

- **Отличный выбор** для большинства задач, включая шифрование изображений, потоковых данных и дисков.
- **Преимущества:**
  - **Распараллеливание:** И шифрование, и расшифрование могут выполняться параллельно, что значительно ускоряет работу на современных процессорах.
  - **Отсутствие распространения ошибок:** Повреждение одного бита шифртекста приведет к повреждению только одного бита открытого текста (в CBC ошибка распространялась бы на весь блок).

### 4.

Размер блока не спасает режим ECB от утечки информации. И при 64-битном, и при 128-битном блоке паттерны будут хорошо видны. Проблема заключается не в размере блока, а в самой концепции режима ECB. **Правильное решение — не использовать ECB**, а использовать режимы с рандомизацией (CBC, CTR), которые полностью решают эту проблему независимо от размера блока.

**Вывод:** Зашифровал предложенные изображения всеми возможными алгоритмами во всех возможных режимах. Провел анализ полученной зашифровки, сделал вывод об эффективности тех или иных режимов зашифровки, а так же в какой ситуации их лучше использовать.