

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 дисциплине

Средства и методы защиты информации в интеллектуальных системах

Выполнил:

А. С. Терлеев

Студент группы

121703

Проверил:

В. В. Захаров

Минск 2023

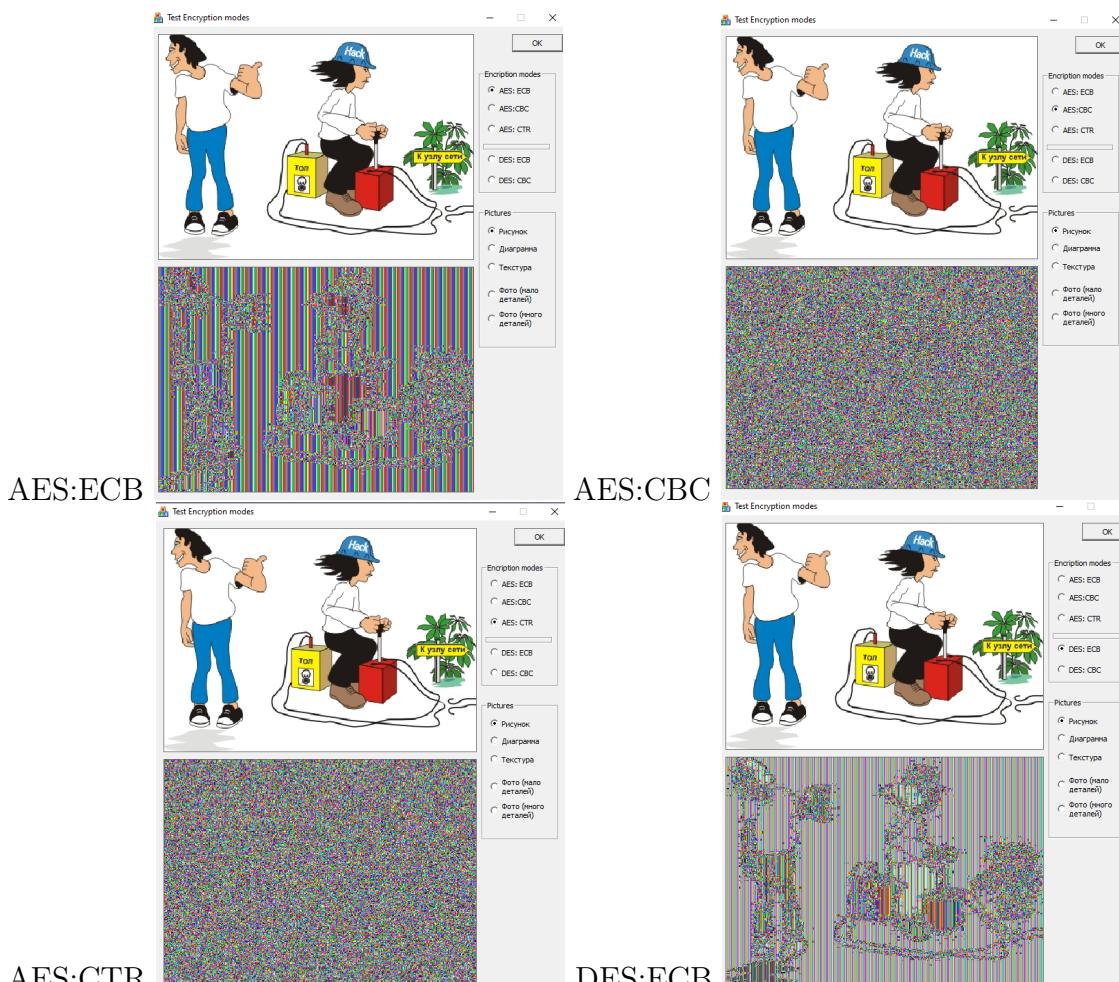
**Тема:** Режимы применения блочных шифров

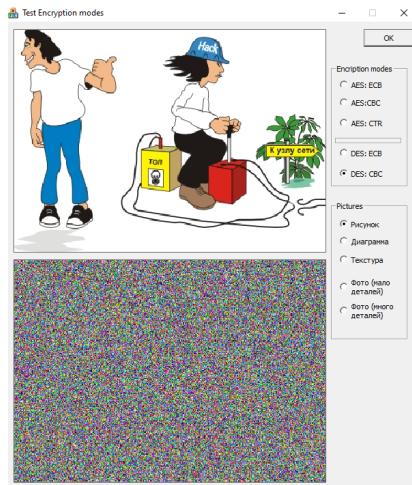
**Задача:**

1. Зашифровать предложенные изображения всеми алгоритмами во всех возможных режимах. Результаты шифрования отразить в отчете в виде скриншотов
2. Оценить полученные результаты о 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 цифрования и почему?

**Выполнение работы:**

Рисунок

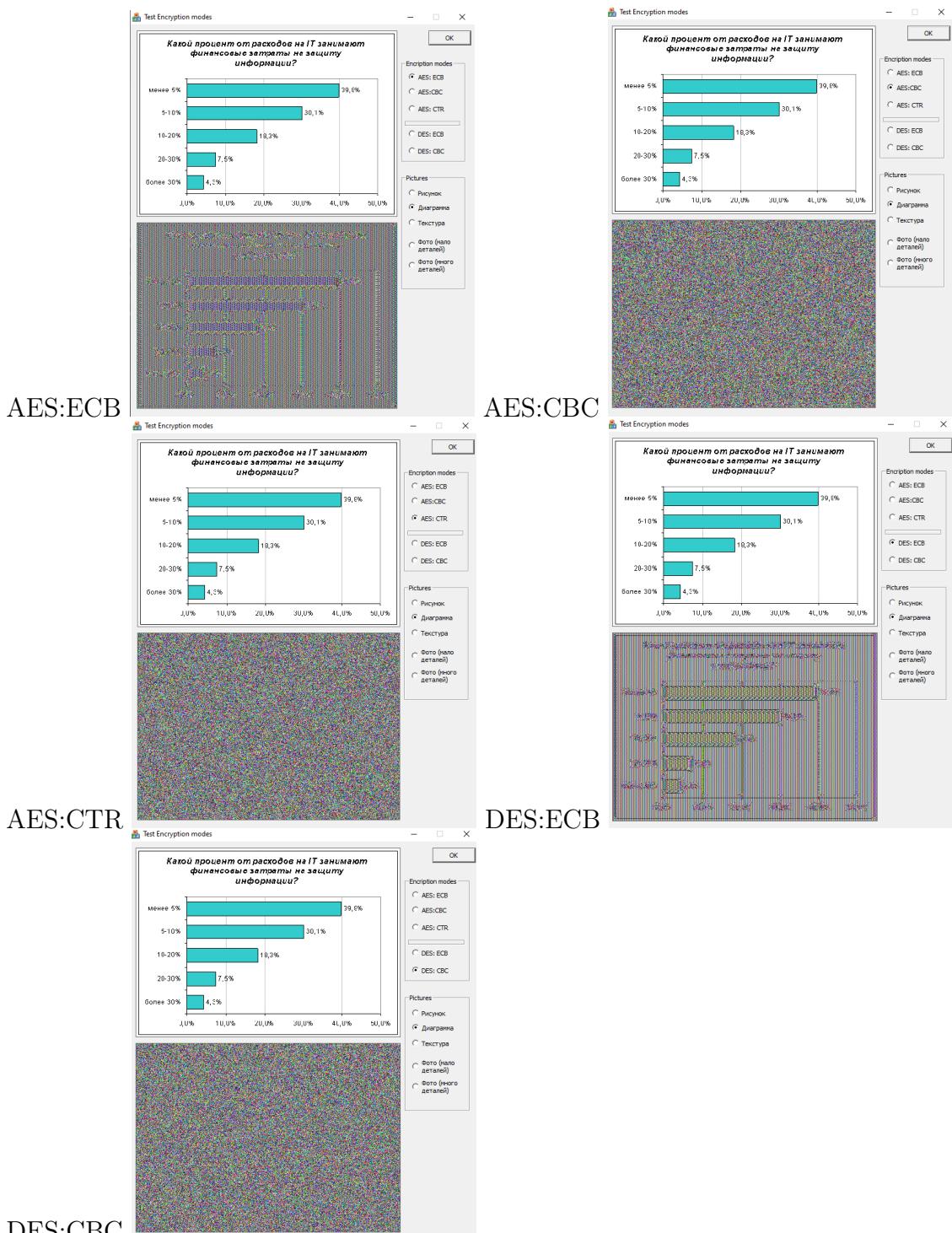




DES:CBC

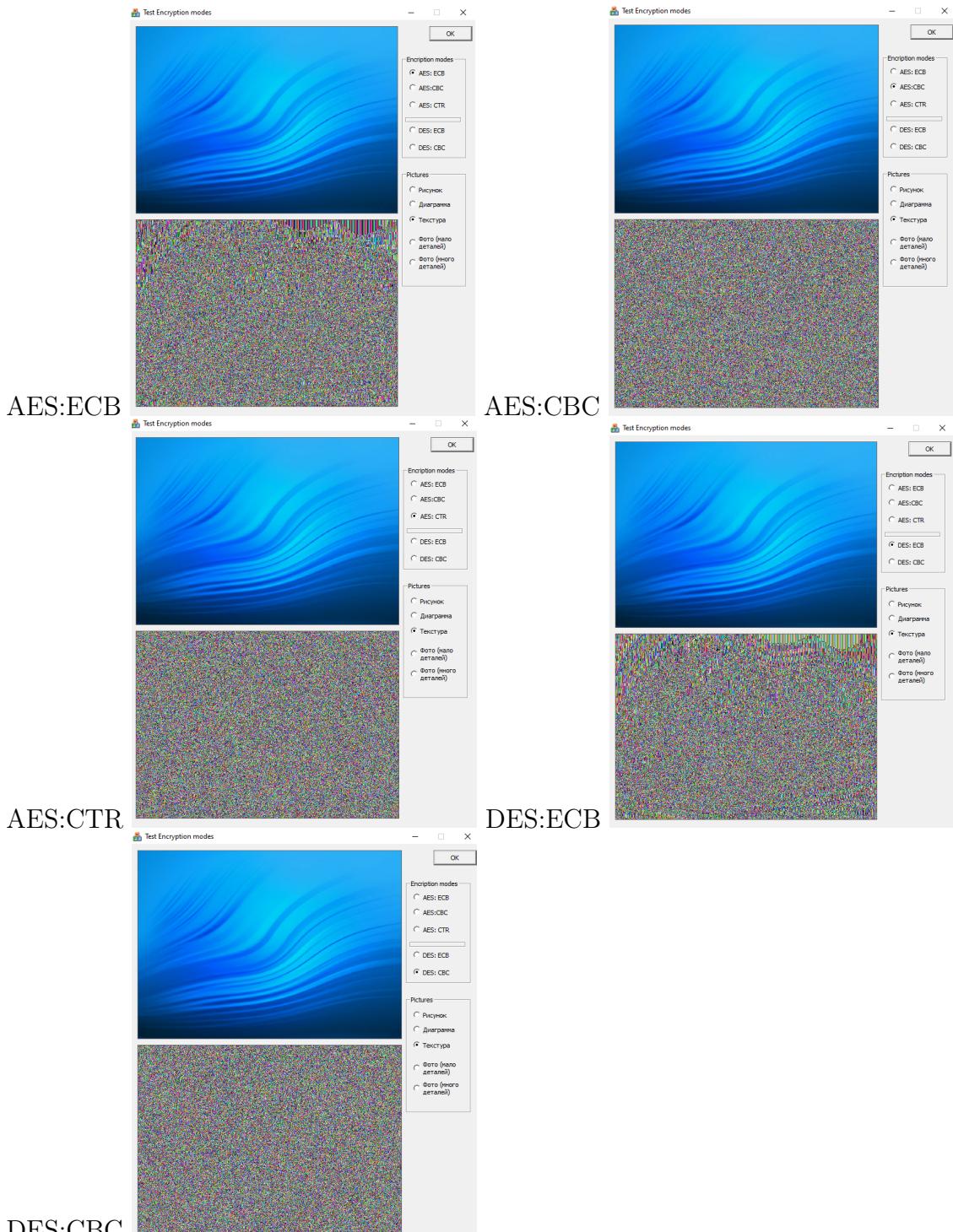
**Вывод:** В режимах шифрования AES:ECB и DES:ECB данные разбиваются на блоки фиксированного размера, и каждый блок шифруется независимо друг от друга. Это приводит к видимости "текстуры" данных, поскольку небольшое количество цветов используется в изображении. В других режимах, таких как CBC, каждый блок данных перед шифрованием комбинируется с предыдущим шифротекстом с использованием операции XOR. В режиме CTR блочный шифр AES преобразуется в потоковый шифр.

## Диаграмма



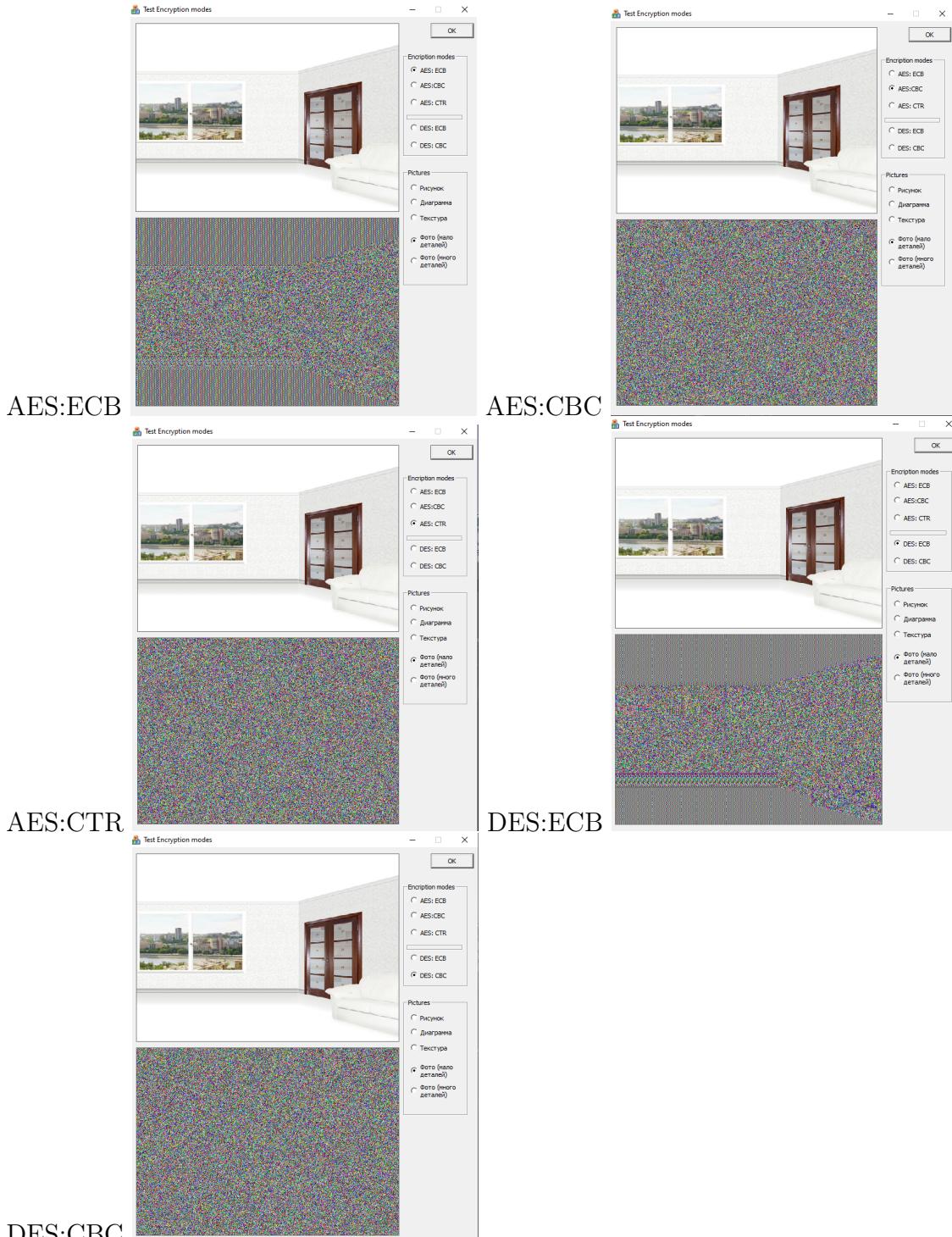
**Вывод:** В случае использования режима шифрования ECB мы можем наблюдать диаграммы, которые были зашифрованы. Однако, поскольку длина блока в шифре DES меньше, чем длина блока в шифре AES, диаграммы, зашифрованные с использованием DES:ECB, становятся более заметными или легче видимыми.

## Текстура



**Выход:** Несмотря на то, что на картинке мало объектов, используется множество различных оттенков цвета, что позволяет нам эффективно применить любой из предложенных шифров для хорошего уровня зашифрованности.

## Фото (мало деталей)



**Выход:** Из-за тех же причин, что и на рисунке, в режиме ECB мы можем видеть силуэты, поскольку каждый блок шифруется независимо от других блоков. Кроме того, на самом рисунке присутствует небольшое количество объектов с ограниченным числом цветов

## Фото (много деталей)



**Выход:** В данном примере все режимы зашифровали хорошо, так как на фото присутствует большое количество деталей и разных оттенков цветов, поэтому невозможно определить даже силуэты

## **Общий вывод и рекомендации:**

Для шифрования изображений, содержащих повторяющиеся элементы или имеющих небольшое количество деталей, рекомендуется использовать режимы CBC и CTR алгоритма AES, а также режим CBC алгоритма DES.

При сравнении режимов CBC(AES) и CBC(DES), наилучшим выбором будет CBC(AES). Оба режима зависят от шифрования всех предыдущих блоков, однако CBC(AES) имеет меньшее количество блоков и сам алгоритм является более эффективным, что обеспечивает более быструю операцию шифрования.

Если сравнивать режимы CBC и CTR, то предпочтительным будет CTR. Режим CTR шифрует текущий блок данных на основе значения счетчика, что позволяет параллельное выполнение операций шифрования и расшифрования и обеспечивает более высокую производительность. Это дает преимущество перед режимом CBC.

Таким образом, для шифрования изображений с повторяющимися элементами или небольшим количеством деталей рекомендуется использовать режим CTR. Этот режим обеспечивает безопасность шифрования и имеет преимущества в производительности.