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 Батук Д.С.

Проверил: Сальников Д.А.

Минск 2025

ЛАБОРАТОРНАЯ РАБОТА № 3 “РЕЖИМЫ ПРИМЕНЕНИЯ БЛОЧНЫХ ШИФРОВ”

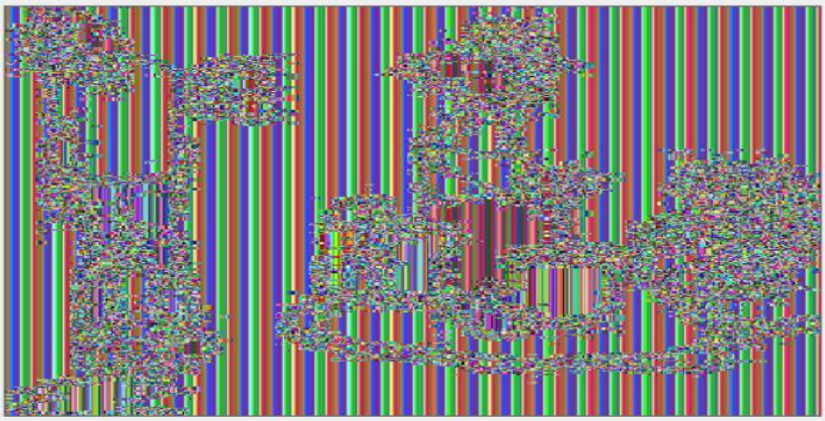
Цель:

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.

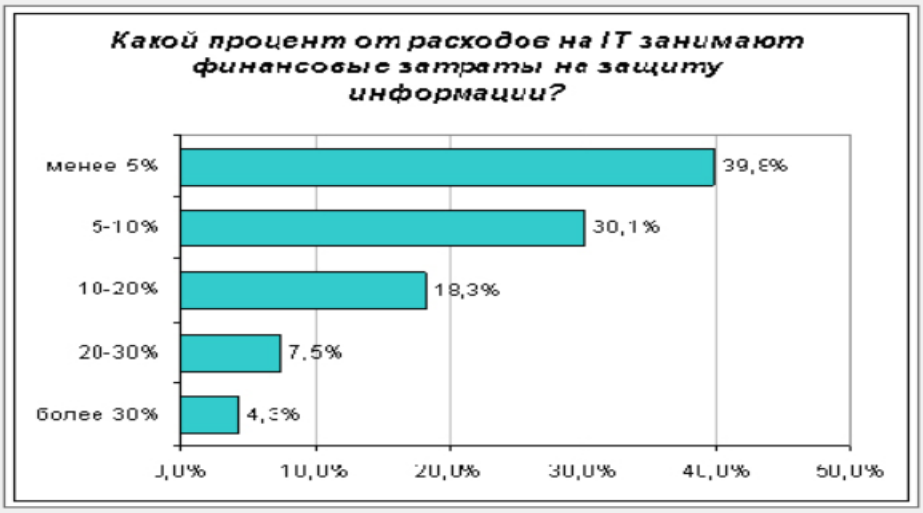
4) Дать ответ на вопрос: как влияет размер блока шифра на результат шифрования и почему?

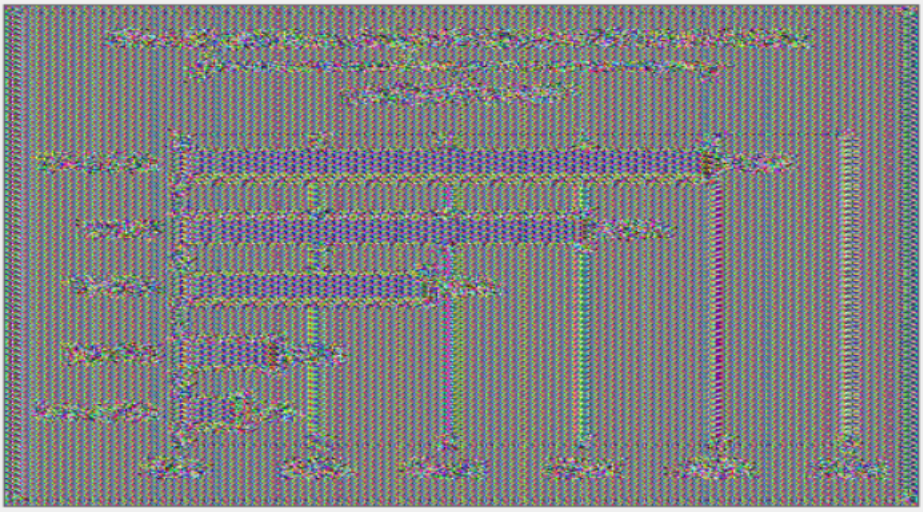


OK

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)

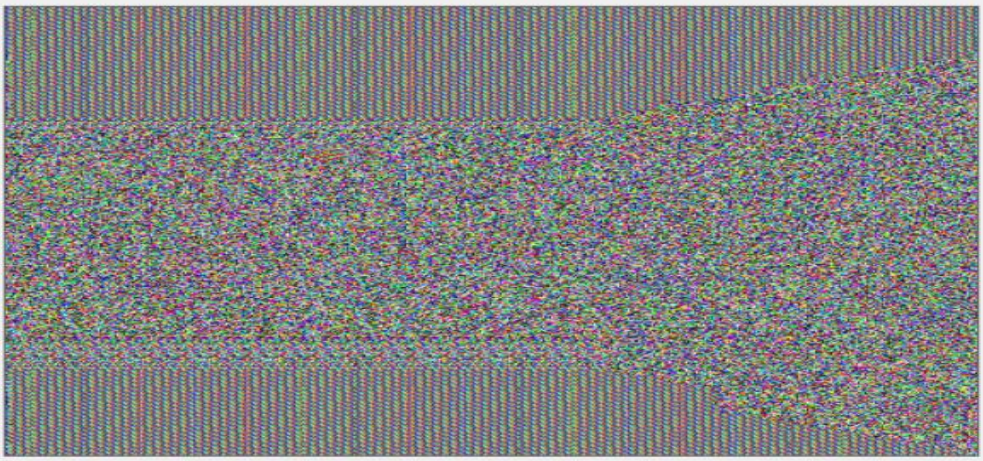
OK

Encription modes

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

Pictures

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



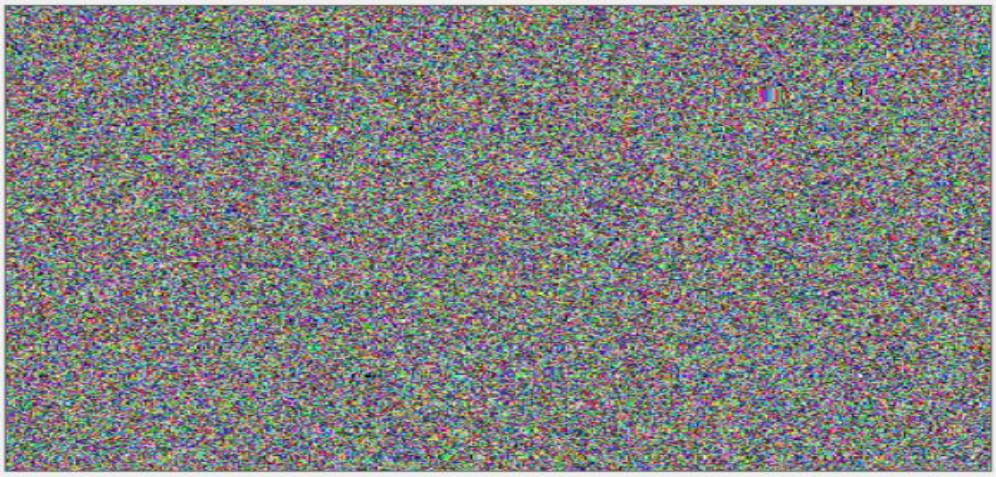
OK

Encription modes

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

Pictures

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



OK

Encription modes

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

Pictures

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

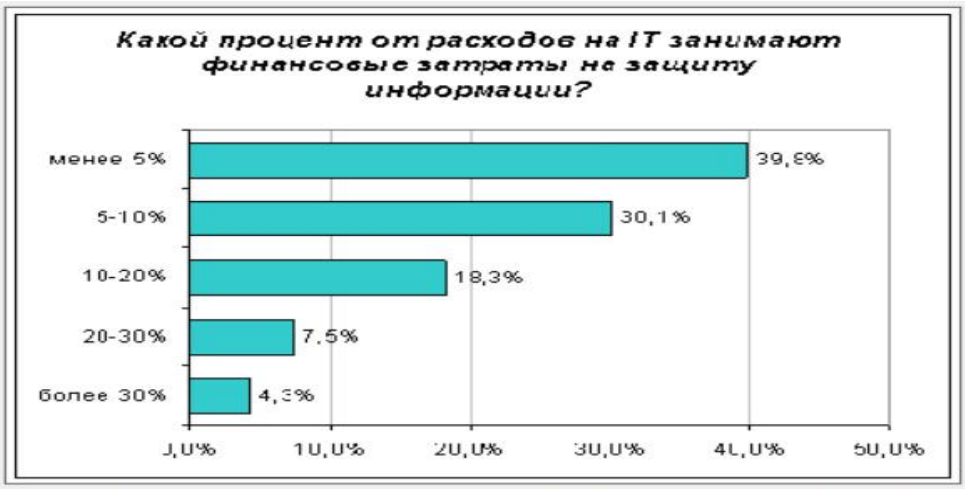
OK

Encription modes

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

Pictures

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



OK

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

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

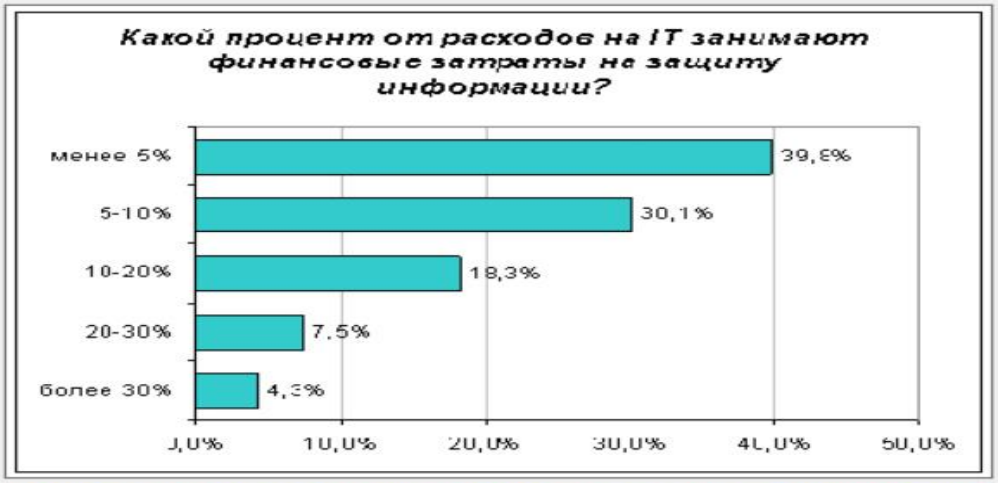
Pictures

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

OK

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

Encription modes

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

Pictures

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

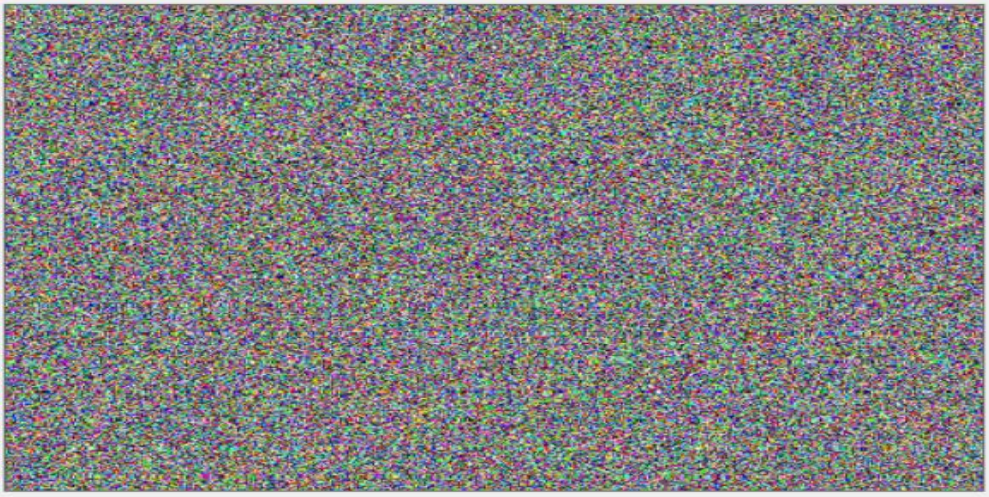
OK

Encription modes

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

Pictures

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



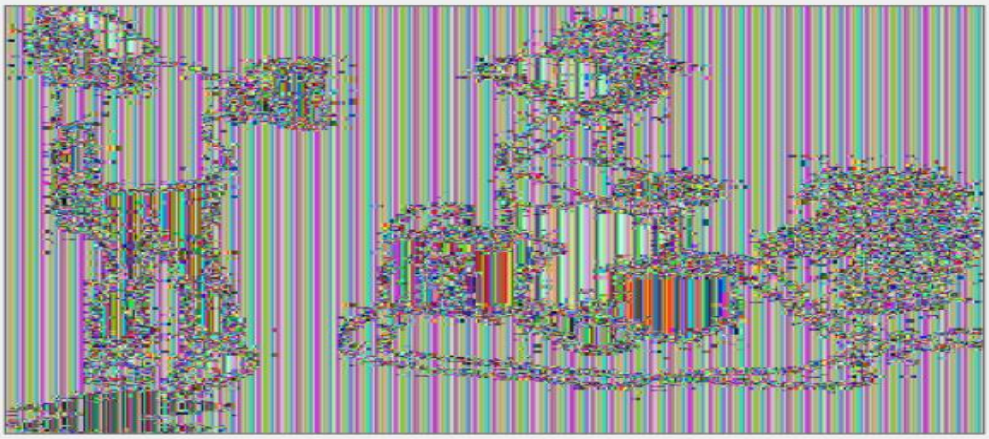
OK

Encription modes

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

Pictures

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



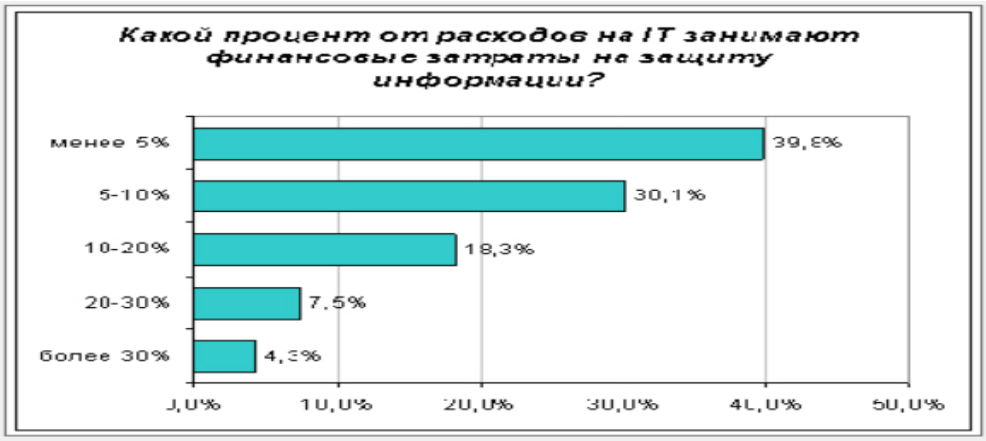
OK

Encription modes

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

Pictures

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



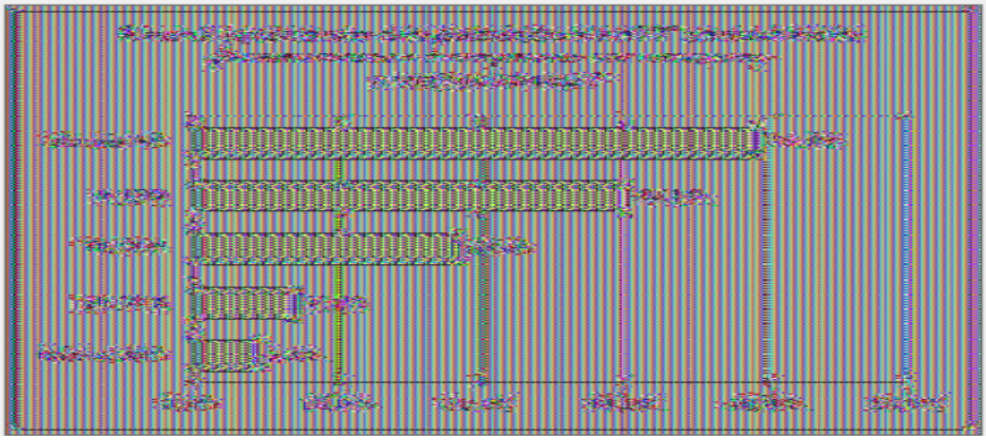
OK

Encription modes

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

Pictures

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



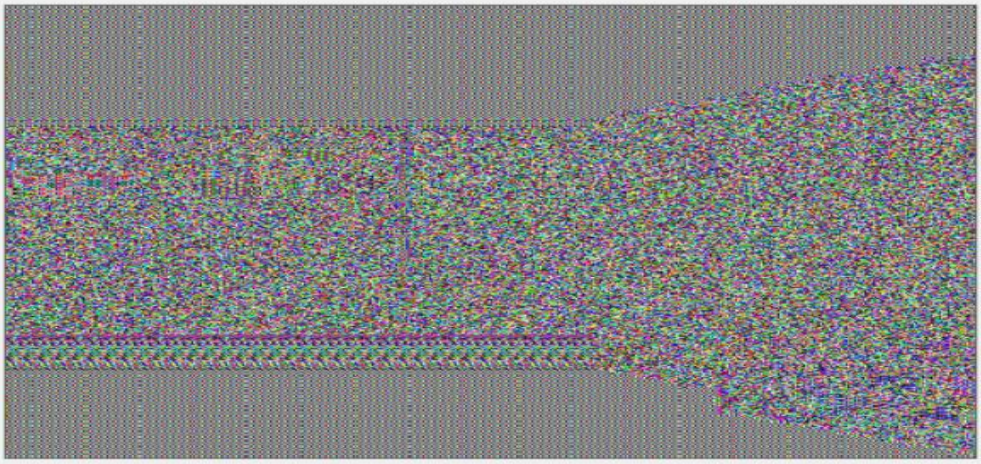
OK

Encription modes

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

Pictures

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



OK

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

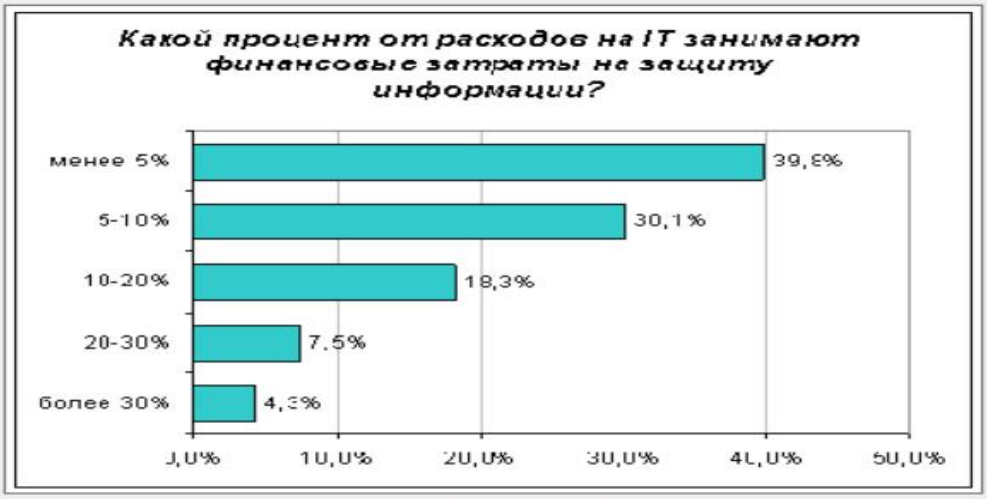
Pictures

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

OK

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)

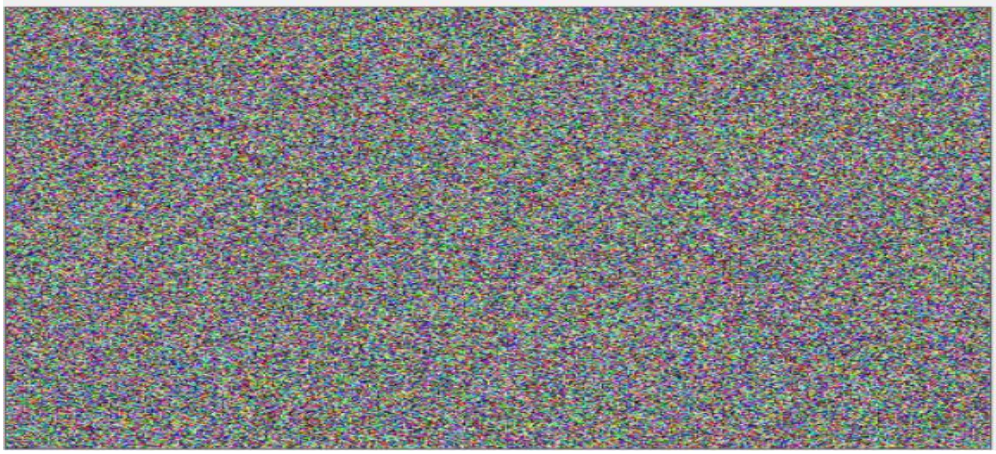
OK

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

Encription modes

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

Pictures

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

2. Оценка результатов и анализ причин

Режим ECB (Electronic Codebook)

- Результат: На зашифрованном изображении отчётливо прослеживаются контуры и общая структура исходного файла. Однородные области и градиенты преобразуются в повторяющиеся узоры.

- Причина: Эта особенность является главным недостатком ECB. Одинаковые блоки данных шифруются в идентичные блоки шифротекста. Поскольку в изображениях часто встречаются большие участки с одинаковыми пикселями (например, белый фон или сплошной цвет), эти области после шифрования сохраняют свою однородность, что делает исходную картинку узнаваемой. Таким образом, шифр не скрывает статистические свойства данных.

Режим CBC (Cipher-Block Chaining)

- Результат: Зашифрованное изображение выглядит как абсолютно случайный шум. Никакие контуры, детали или узнаваемые элементы не просматриваются.

- Причина: Каждый блок исходных данных перед шифрованием комбинируется с предыдущим зашифрованным блоком (операция XOR). Это обеспечивает уникальность шифротекста для каждого блока, даже если исходные блоки были идентичны. Эффект "сцепления" распространяет изменения по всему шифротексту, полностью уничтожая любые видимые паттерны.

Режим CTR (Counter)

- Результат: Как и в случае с CBC, зашифрованное изображение представляет собой хаотичный набор пикселей без каких-либо видимых закономерностей.

- Причина: Данный режим работает как поточный шифр. Шифруется не сам блок данных, а уникальное значение счётчика. Затем результат XOR-операцией накладывается на исходный текст. Поскольку значение счётчика всегда уникально, одинаковые блоки исходных данных будут зашифрованы по-разному, что исключает появление паттернов.

Сравнение алгоритмов AES и DES

- Визуальная разница: В рамках надёжных режимов (CBC или CTR) визуально различить AES и DES невозможно. Оба алгоритма преобразуют изображение в случайный шум .

- Криптографическая стойкость: Основное отличие — в безопасности. DES с 56-битным ключом устарел и может быть взломан полным перебором на современном оборудовании. AES (ключи 128/192/256 бит) — это современный и надёжный стандарт, обеспечивающий высокий уровень криптостойкости.

3. Рекомендации

Выбор алгоритма

- AES: Безальтернативный выбор для любых новых систем и приложений. Полностью соответствует современным требованиям безопасности.

- DES: Не рекомендуется для защиты новых данных. Его использование оправдано только для обеспечения совместимости со старыми, легаси-системами.

Выбор режима

- ECB: Непригоден для шифрования данных с избыточностью (изображения, видео), так как раскрывает статистические свойства. Его применение крайне ограничено, например, для шифрования уже зашифрованных или случайных данных, которые по своей природе не содержат паттернов.

- CBC: Хороший выбор для шифрования файлов и данных в потоковом режиме. Недостаток: Операции шифрования не могут быть распараллелены, поскольку каждый блок зависит от предыдущего. Требуется надёжный механизм передачи уникального вектора инициализации (IV).

- CTR: Отличный выбор для большинства современных задач, включая потоковое шифрование и шифрование дисков. Ключевые преимущества:

    - Высокая производительность: Шифрование и расшифрование могут быть распараллелены, что значительно ускоряет работу на многоядерных процессорах.

    - Сопротивление ошибкам: Повреждение одного бита шифротекста приведёт к повреждению только одного бита исходного текста.

Дополнительный вывод

Размер блока не решает фундаментальную проблему режима ECB. Паттерны будут заметны как при 64-битном, так и при 128-битном размере блока. Проблема заключается не в размере блока, а в самой концепции режима, лишённого рандомизации. Правильным решением является выбор режимов, использующих рандомизацию (CBC, CTR), которые полностью устраняют эту проблему.

Вывод

В рамках проведённого эксперимента я зашифровал изображения с использованием различных алгоритмов и режимов, проанализировал результаты и сделал вывод об эффективности каждого из них, а также определил оптимальные сценарии их применения.