Лекция 8.
Методы и модели кибербезопасности в современном информационном обществе

Методы резервирования информации

Методы резервирования информации

По *времени восстановления*

оперативные

неоперативные методы

Методы резервирования информации

По *числу копий*

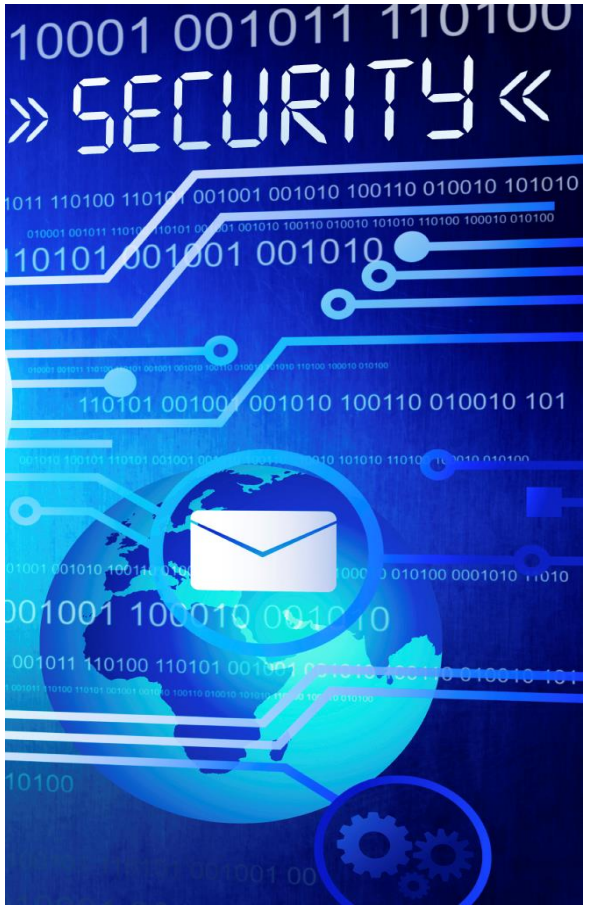
По *степени пространственной удаленности носителей основной*

сосредоточенные и *рассредоточенные* методы.

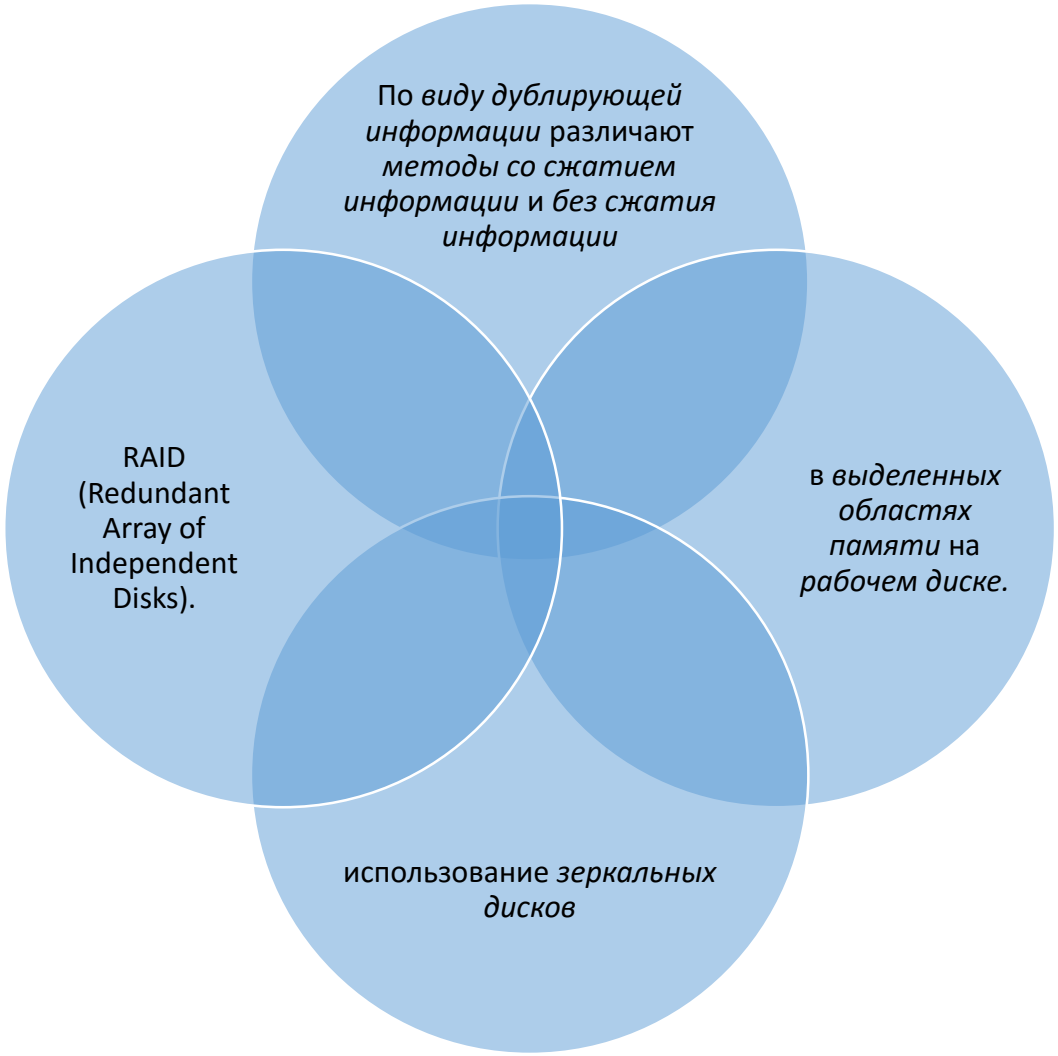
с процедурой дублирования

полного копирования, зеркального копирования, частичного копирования, комбинированного копирования

По *виду дублирующей информации* различают *методы со сжатием информации* и *без сжатия информации*



Методы резервирования информации



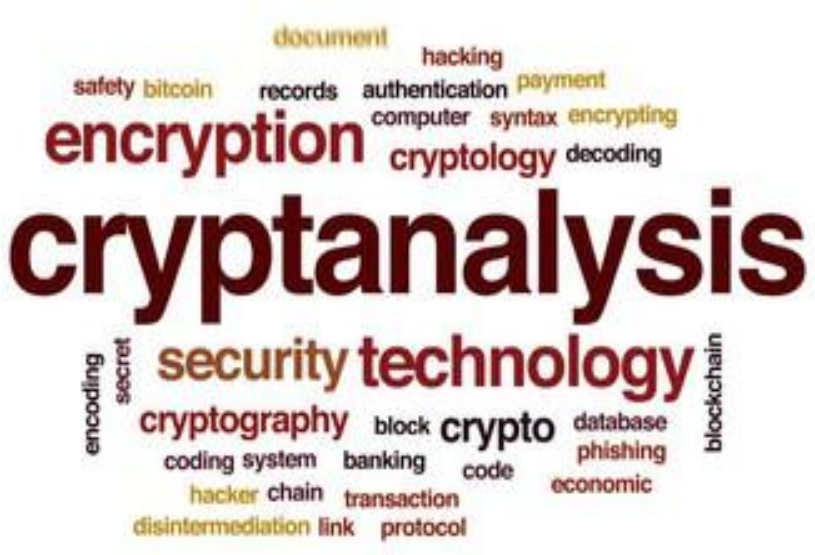
Методы резервирования информации

Тестировать

Резервное копирование

- дата выполнения дублирования;
- номер накопителя;
- тип выполняемого дублирования;
- компьютер, данные которого дублируются;
- имена сохраненных файлов;
- фамилия сотрудника, выполняющего операцию;
- местонахождение накопителя с резервной копией.

Аппаратно-программные средства защиты информации



Классификация методов дублирования

Защита информации в КС от несанкционированного доступа (НСД)

Защита информации в КС от несанкционированного доступа (НСД)

1. несанкционированный доступ к сетям и сетевым ресурсам;

2. раскрытие и модификация данных и программ;

3. раскрытие, модификация и подмена трафика.

Несанкционированный доступ к сетям и сетевым ресурсам

1) Применение компьютеров, не имеющих парольной защиты во время загрузки;

2) Использование совместных и легко вскрываемых паролей;

3) Хранение паролей в пакетных файлах и на дисках компьютеров;

4) Отсутствие установления подлинности пользователя в реальном масштабе времени;

5) Отсутствие или низкая эффективность применения систем идентификации и аутентификации пользователей;

6) Недостаточность физического контроля за сетевыми устройствами;

7) Отсутствие отключения терминала при многочисленных неудачных попытках установления сети связи и регистрации таких попыток;

8) Незащищенность модемов.

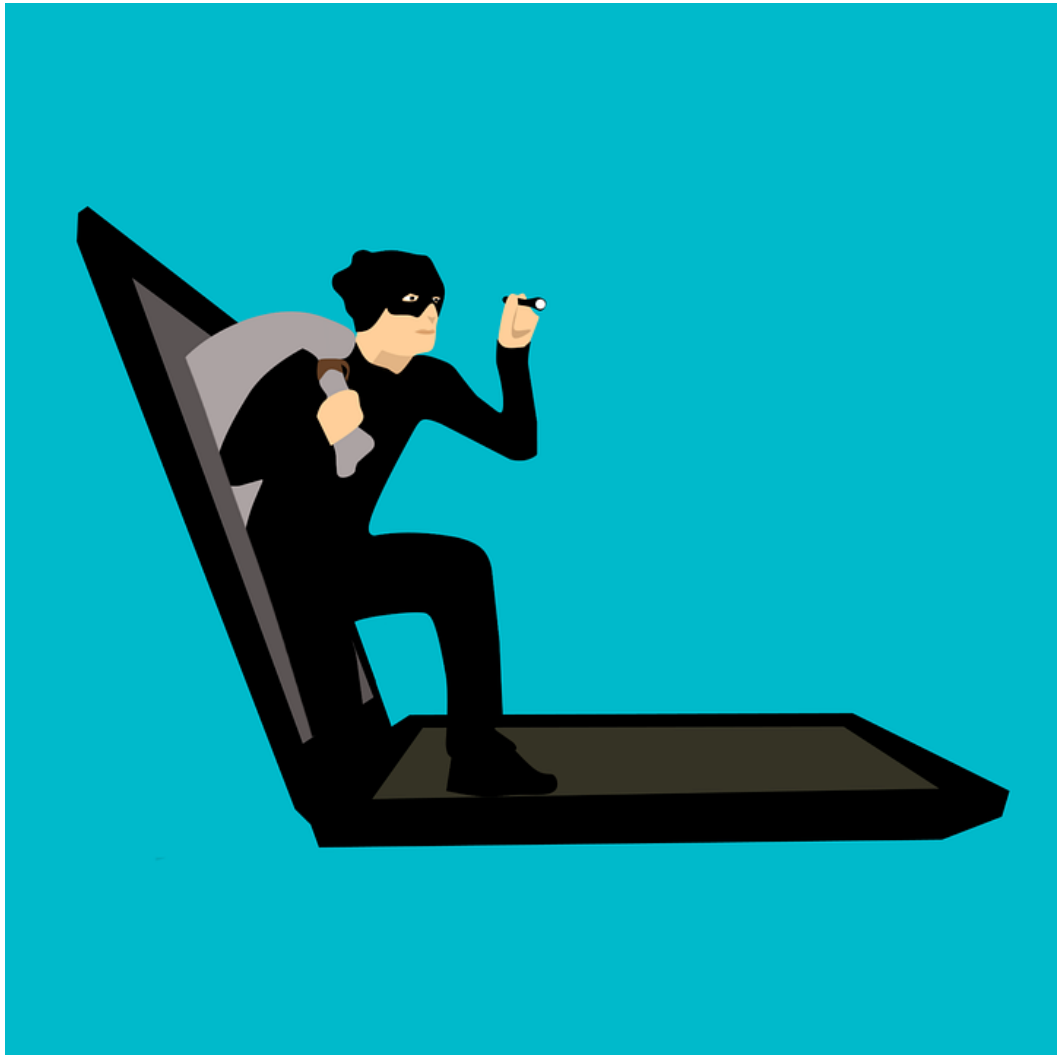
Несанкционированный доступ к сетям и сетевым ресурсам

- Пароли, устанавливаемые пользователем;
- Пароли, генерируемые системой;
- Случайные коды доступа, генерируемые системой;
- Полуслова;

Несанкционированный доступ к сетям и сетевым ресурсам

- Ключевые фразы;
- Интерактивные последовательности типа «вопрос- ответ»;
- «Строгие» пароли.

Несанкционированный доступ к сетям и сетевым ресурсам



Раскрытие и модификация данных и программ

Раскрытие, модификация и подмена трафика

Понятие о системах идентификации и аутентификации

Идентификация

Аутентификация

Атрибутивный

Понятие о системах идентификации и аутентификации

пластиковая карта

биометрической идентификации

электронной цифровой подписи (ЭЦП).

Модели защиты информации

доступа только для чтения

При полном доступе

При доступе в зависимости от пароля

Права доступа

ПРАВО	ЗНАЧЕНИЕ
Read	Чтение и копирование файлов из совместно используемого каталога.
Execute	Запуск (выполнение) программ из каталога.
Write	Создание новых файлов в каталоге.
Delete	Удаление файлов в каталоге.
No Access	Запрещение на доступ к каталогу, файлу или ресурсу.

Криптографические методы защиты информации

в ***системах обработки и передачи*** информации.

применяются криптографические методы защиты информации,

Процесс шифрования

<u>алгоритм преобразования</u> и <u>ключ</u>.

Криптографические методы защиты информации

Методы стеганографии

Кодирования информации

Сжатие

Понятие о шифре и ключе, о шифровании и дешифровании. Их характеристики и требования, предъявляемые к ним

- криптостойкость (противостояние криптоанализу) должна быть такой, чтобы вскрытие шифра могло быть осуществлено только путем решения задачи полного перебора ключей;

- криптостойкость обеспечивается не секретностью алгоритма шифрования, а секретностью ключа;

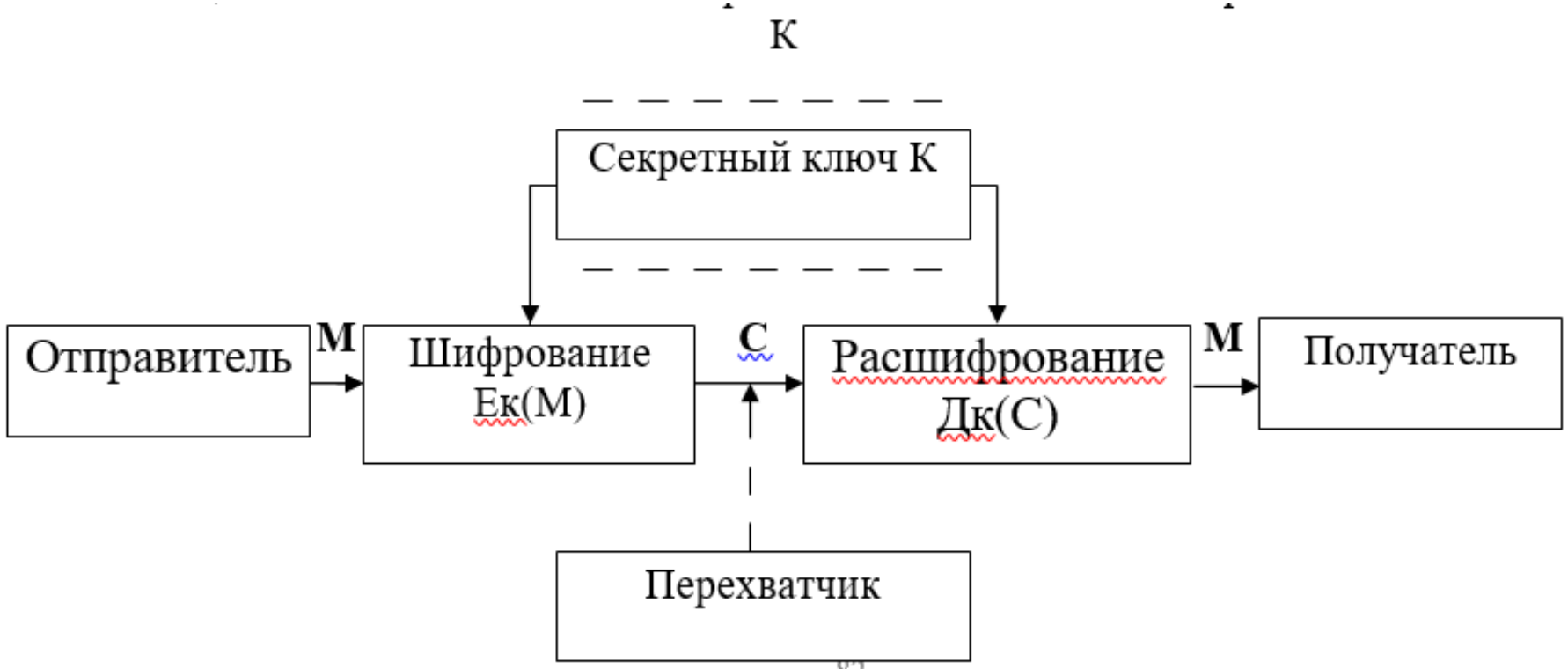
- шифротекст не должен существенно превосходить по объему исходную информацию;

- ошибки шифрования не должны приводить к искажениям и потерям информации;

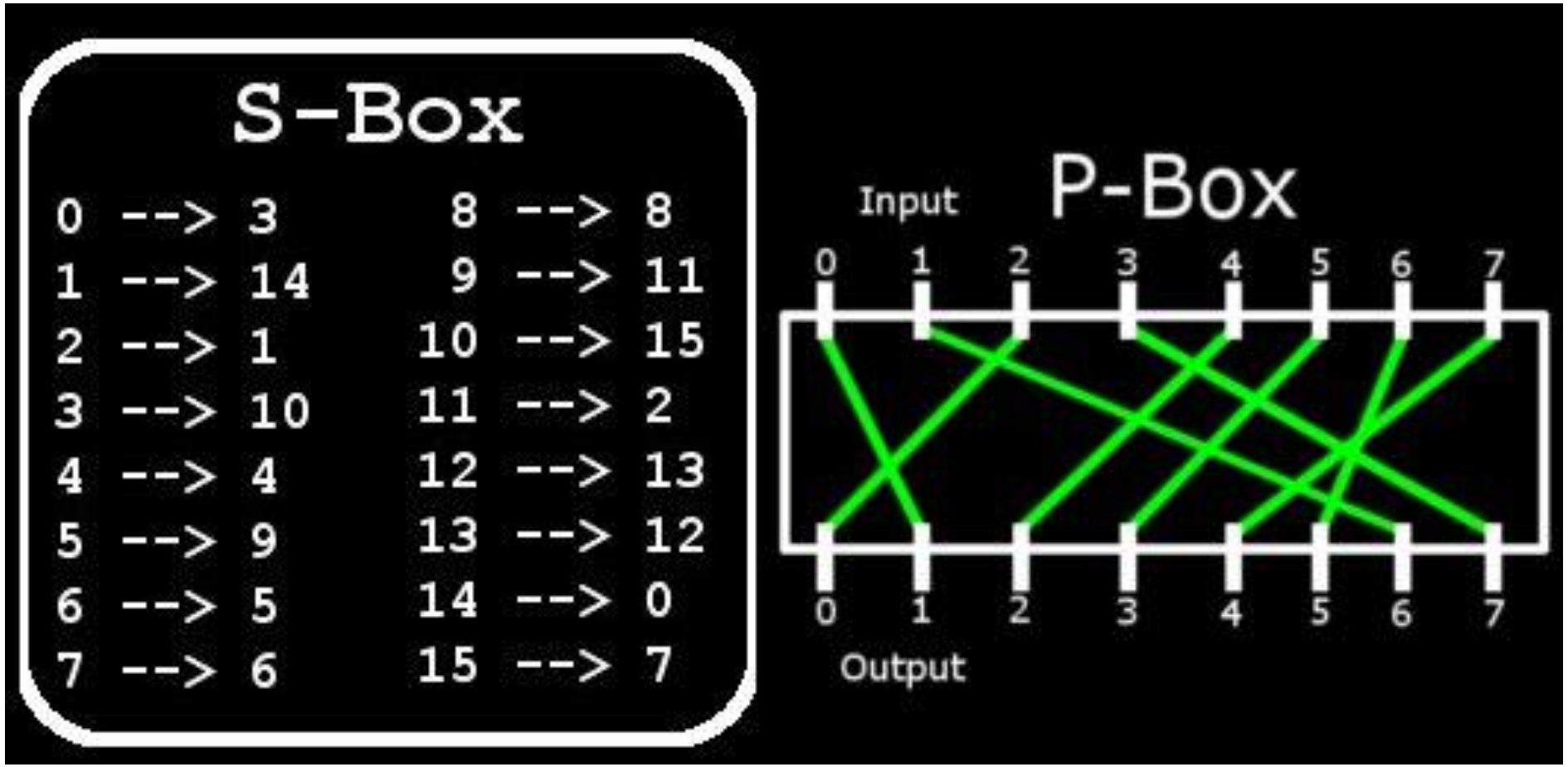
время шифрования не должно быть большим;

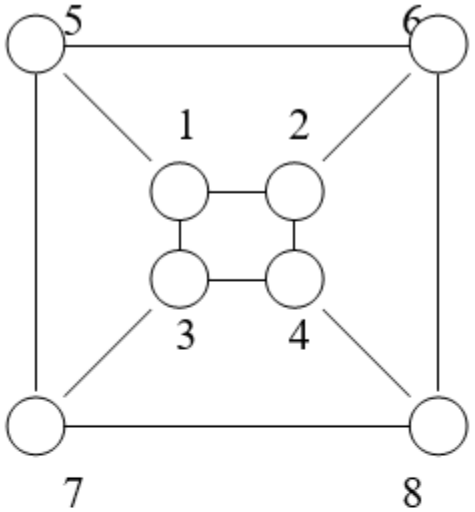
стоимость должна быть согласована со стоимостью закрываемой информации.

Классические схемы и модели функционирования криптосистемы

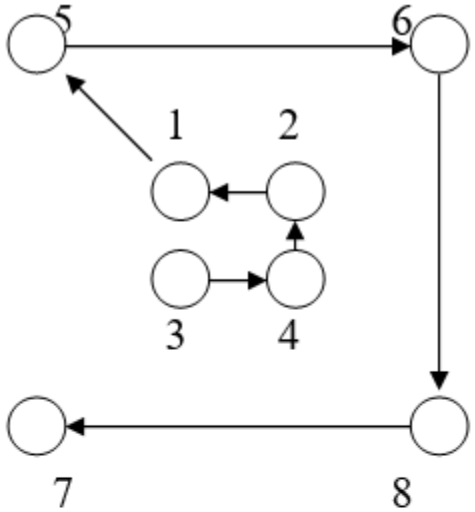


Методы симметричного и асимметричного шифрования

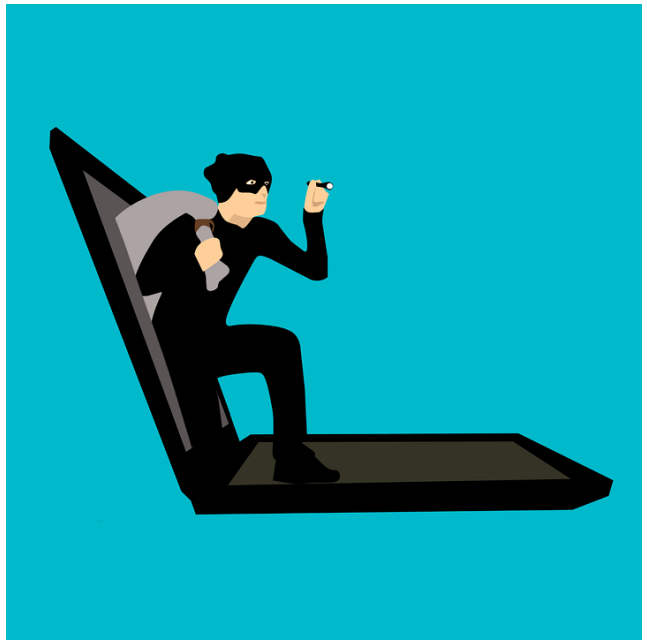


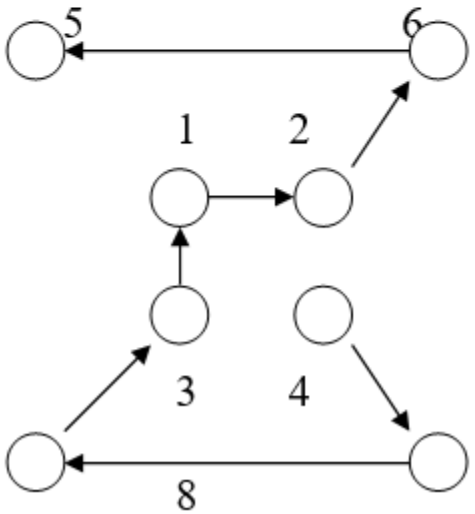


Таблица



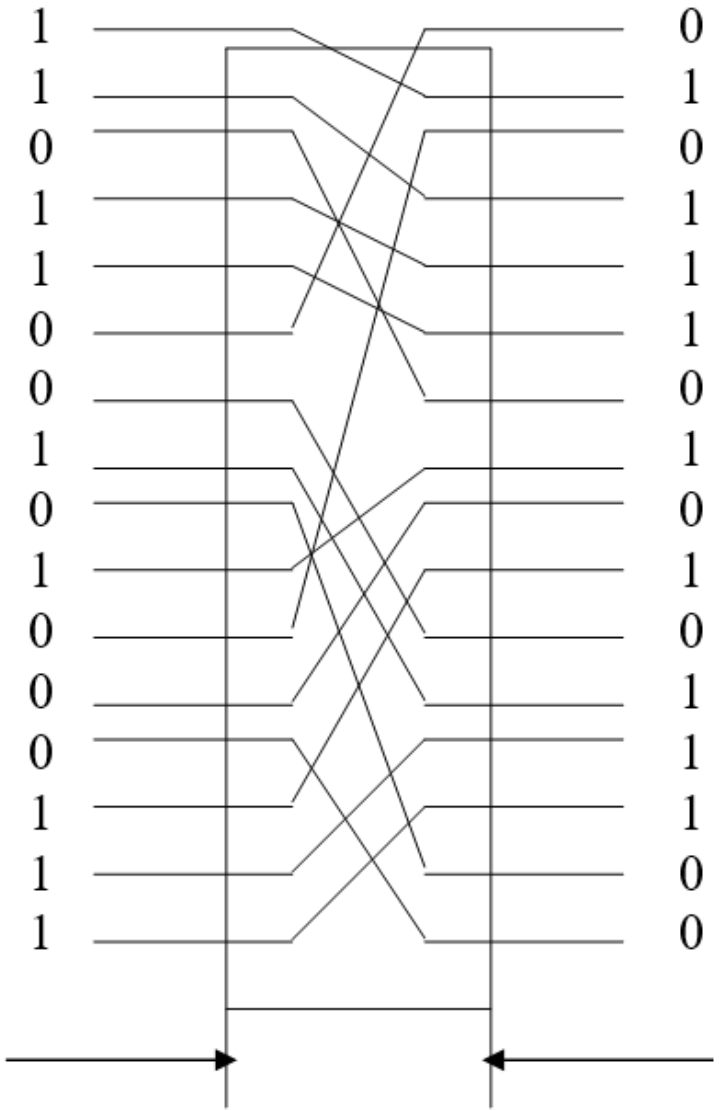
Маршрут №1





Метод перестановки

Зашифрование Расшифрование



Зашифрование Расшифрование

Аналитические методы

Матричная алгебра

Аддитивные методы шифрования (гаммирование)

Открытый ключ

Стеганография