

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

МЕТОДЫ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ

Перечень учебных вопросов.

- 1. Угрозы ЦИ
- 2. Методы обеспечения ЦИ
- 3. Виды кодирования.
- 2. Код Хемминга
- 3. Методы оптимального кодирования

Угрозы ЦИ

Исходя из определения ЦИ, можно выделить следующие воздействия на информацию:

- модификация информации;
- подмена информации;
- уничтожение информации.

- Модификация предполагает изменения какой-либо части информации. Эти изменения может быть как случайным, так и преднамеренным. Во втором случае они могут быть санкционированными либо несанкционированными.

- Подмена предполагает навязывание ложной информации путем замены истинной (первоначальной) информации.
- Уничтожение чаще всего связывается с уничтожением физического носителя информации и/или размагничиванием (форматированием) электронных носителей.

ВОЗМОЖНЫЕ УГРОЗЫ ЦИ В ТЕЧЕНИЕ ЕЕ ЖИЗНЕННОГО ЦИКЛА

- При использовании неполных и/или ложных данных во время создания (появления) информации можно получить не соответствующую действительности информацию о тех или иных событиях.

- При обработке информации нарушение ЦИ может возникнуть вследствие технических неисправностей, алгоритмических и программных ошибок, ошибок и деструктивных действий обслуживающего персонала, внешнего вмешательства, действия разрушающих и вредоносных программ (вирусов, эксплойтов, червей, логических бомб).

- В процессе передачи информации могут воздействовать различного рода помехи как естественного, так и искусственного происхождения. При этом возможно ее искажение или стирание (уничтожение). Кроме этого, возможен перехват информации с целью ее модификации и дальнейшего навязывания.

- В процессе хранения основными угрозами являются несанкционированный доступ с целью модификации (вплоть до уничтожения) информации, вредоносные программы (вирусы, трояны, черви, логические бомбы) и технические неисправности.

- В процессе старения основными угрозами информации, наряду с угрозами при хранении, можно считать утерю технологий, способных воспроизвести ту или иную информацию, и физическое старение носителей информации.

Методы обеспечения ЦИ

- Надежность технических средств
- Помехоустойчивое кодирование
- Разграничение доступа
- Антивирусная защита
- Стеганография
- Сжатие данных
- Резервирование

Классы помехоустойчивых кодов

- Жесткое декодирование
 - Коды с обнаружением ошибок
 - Коды с исправлением ошибок
- Мягкое декодирование

Коды с обнаружением ошибок

- Проверка на четность
- Проверка на нечетность

Код Хемминга

- Одним из наиболее известных кодов, систематических кодов является код Хэмминга. Кодом Хэмминга называется (n, k) -код, проверочная матрица которого имеет $r = n - k$ строк и $2^r - 1$ столбцов, причем столбцами являются все различные ненулевые последовательности.
- **Это один из наиболее используемых кодов, исправляющие однократные ошибки.**

Длина кодовой комбинации

$$n = k + r,$$

где k - количество информационных разрядов;

r - количество проверочных разрядов.

$$H_{(15,4)} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \mathbf{u}_1 & \mathbf{u}_2 & \mathbf{u}_3 & \mathbf{u}_4 & \mathbf{u}_5 & \mathbf{u}_6 & \mathbf{u}_7 & \mathbf{u}_8 & \mathbf{u}_9 & \mathbf{u}_{10} & \mathbf{u}_{11} & \mathbf{u}_{12} & \mathbf{u}_{13} & \mathbf{u}_{14} & \mathbf{u}_{15} \end{bmatrix}$$

$$H_{(15,4)} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ \mathbf{a}_1 & \mathbf{a}_2 & \mathbf{a}_3 & \mathbf{a}_4 & \mathbf{a}_5 & \mathbf{a}_6 & \mathbf{a}_7 & \mathbf{a}_8 & \mathbf{a}_9 & \mathbf{a}_{10} & \mathbf{a}_{11} & \mathbf{b}_1 & \mathbf{b}_2 & \mathbf{b}_3 & \mathbf{b}_4 \end{bmatrix}$$

$$\begin{cases} b_1 = a_5 + a_6 + a_7 + a_8 + a_9 + a_{10} + a_{11} \\ b_2 = a_2 + a_3 + a_4 + a_8 + a_9 + a_{10} + a_{11} \\ b_3 = a_1 + a_3 + a_4 + a_6 + a_7 + a_{10} + a_{11} \\ b_4 = a_1 + a_2 + a_4 + a_5 + a_7 + a_9 + a_{11} \end{cases}$$

$$\begin{cases} S_1 = u_1 + u_3 + u_5 + u_7 + u_9 + u_{11} + u_{13} + u_{15} \\ S_2 = u_2 + u_3 + u_6 + u_7 + u_{10} + u_{11} + u_{14} + u_{15} \\ S_3 = u_4 + u_5 + u_6 + u_7 + u_{12} + u_{13} + u_{14} + u_{15} \\ S_4 = u_8 + u_9 + u_{10} + u_{11} + u_{12} + u_{13} + u_{14} + u_{15} \end{cases}$$

- Сообщение

- 110 0101 0110 ($k = 11$)

- Криптограмма

- { u_1u_2 u_4 100 u_8 101 0110 }

$$\begin{cases} \mathbf{u}_1 = \mathbf{u}_3 + \mathbf{u}_5 + \mathbf{u}_7 + \mathbf{u}_9 + \mathbf{u}_{11} + \mathbf{u}_{13} + \mathbf{u}_{15} \\ \mathbf{u}_2 = \mathbf{u}_3 + \mathbf{u}_6 + \mathbf{u}_7 + \mathbf{u}_{10} + \mathbf{u}_{11} + \mathbf{u}_{14} + \mathbf{u}_{15} \\ \mathbf{u}_4 = \mathbf{u}_5 + \mathbf{u}_6 + \mathbf{u}_7 + \mathbf{u}_{12} + \mathbf{u}_{13} + \mathbf{u}_{14} + \mathbf{u}_{15} \\ \mathbf{u}_8 = \mathbf{u}_9 + \mathbf{u}_{10} + \mathbf{u}_{11} + \mathbf{u}_{12} + \mathbf{u}_{13} + \mathbf{u}_{14} + \mathbf{u}_{15} \end{cases}$$

$$u_1 = 1 + 1 + 0 + 1 + 1 + 1 + 0 = 1$$

$$u_2 = 1 + 0 + 0 + 0 + 1 + 1 + 0 = 1$$

$$u_3 = 1 + 0 + 0 + 0 + 1 + 1 + 0 = 1$$

$$u_4 = 1 + 0 + 1 + 0 + 1 + 1 + 0 = 0$$

Криптограмма

111 1100 0101 0110

Допустим ошибку

111 1110 0101 0110

$$\begin{cases} S_1 = u_1 + u_3 + u_5 + u_7 + u_9 + u_{11} + u_{13} + u_{15} = 0 \\ S_2 = u_2 + u_3 + u_6 + u_7 + u_{10} + u_{11} + u_{14} + u_{15} = 1 \\ S_3 = u_4 + u_5 + u_6 + u_7 + u_{12} + u_{13} + u_{14} + u_{15} = 1 \\ S_4 = u_8 + u_9 + u_{10} + u_{11} + u_{12} + u_{13} + u_{14} + u_{15} = 0 \end{cases}$$

Помехоустойчивый код методом перебора

- Идея кода возникла при рассмотрении цифровой подписи.
- 1 шаг –используя проверку на четность отыскивается искаженный бит в миниблоке размером 4 бита.
- 2 шаг – перебираются возможные варианты построения последовательностей, используя контрольную сумму.

| Десятичное представление | Двоичное представление | Символы алфавита 1 | Символы алфавита 2 | Символы алфавита 3 | Символы алфавита 4 | Символы алфавита 5 |
|--------------------------|------------------------|--------------------|--------------------|--------------------|--------------------|--------------------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 0 | 000 000 | а | а | а | α | 0 |
| 1 | 000 001 | б | б | б | β | 1 |
| 2 | 000 010 | в | в | с | χ | 2 |

| | | | | | | |
|----|---------|-------------|-------------|-------------|--------------|--------------|
| 45 | 101 101 | .пробел | .пробел | .пробел | .пробел | .пробел |
| 46 | 101 110 | . | . | . | . | . |
| 47 | 101 111 | Все строчн. | Все строчн. | Все строчн. | Все строчнн. | Все строчнн. |

| | | | | | | |
|----|---------|------------------|------------------|------------------|------------------|------------------|
| 51 | 110 011 | | Пер-д к алфав. 1 | Пер-д к алфав. 1 | Пер-д к алфав. 1 | Пер-д к алфав. 1 |
| 63 | 111 111 | Пер-д к алфав. 5 | Пер-д к алфав. 5 | Пер-д к алфав. 5 | Пер-д к алфав. 5 | ⊕ |

- $a_1 \oplus a_2 \oplus a_3 = a_4$ – проверка на четность
- $A_i = a_1 a_2 a_3 a_4$ – мини блок
- $A = A_1 A_2 \dots A_k$ – передаваемая последовательность
- $A \bmod 11 = 4$ бита – C1
- $A \bmod 13 = 4$ бита – C2
- $A \bmod 14 = 4$ бита – C3
- $A \bmod 15 = 4$ бита – C4
- C1 C2 C3 C4 – контрольная сумма