МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

ЛЕКЦИОННЫЕ МАТЕРИАЛЫ

Методы обеспечения целостности информации

(наименование дисциплины (модуля) в соответствии с учебным планом)

Уровень	бакалавриат
	(бакалавриат, магистратура, специалитет)
Форма обучения	очная
	(очная, очно-заочная, заочная)
Направление(-я) подготовки	09.03.02 «Информационные системы и технологии»
	(код(-ы) и наименование(-я))
Институт	кибербезопасности и цифровых технологий (ИКБ)
	(полное и краткое наименование)
Кафедра	Разработка программных решений и системное программирование
	(полное и краткое наименование кафедры, реализующей дисциплину (модуль))
Лектор	К.т.н. Ермакова Алла Юрьевна
	(сокращенно – ученая степень, ученое звание; полностью – ФИО)

Используются в данной редакции с учебного года 2023/24

(учебный год цифрами)

Проверено и согласовано «____» _____2023_г.

(подпись директора Института/Филиала с расшифровкой)

Москва 2023 г.

Лекция 6. Протоколы контроля целостности. Проверка четности. Использование контрольных цифр.

Протокол «Проверка четности»

Протокол «Проверка четности» представляет собой самый простой способ обеспечения целостности при хранении или передаче данных. Битовая строка (обычно длиной 7-8 бит), контроль которой необходимо выполнить, дополняется одним, так называемым **паритетным битом** (англ. parity bit). Существует две разновидности проверки четности: с **четным (even)** и **нечетным (odd)** паритетным битом. В первом случае при записи или пересылке данных паритетный бит устанавливается равным 1, если количество единиц в контролируемой строке нечетное, и 0 – если четное. В случае нечетного паритетного бита поступают наоборот.

Таблица 1

Примеры установки бита четности

Битовая строка	Паритетный бит	
	четный (even)	нечетный (odd)
1100 1011	1	0
1001 1001	0	1
1111 1111	0	1
0000 0000	0	1

Недостатки:

- исправление ошибки невозможно;

- в случае изменения состояния четного количества бит (например, двух), вычисленный паритетный бит совпадет с записанным. Т.е. ошибка не будет обнаружена. В то же время, согласно статистики, приблизительно 90% всех ошибок памяти происходит именно с одиночным разрядом. Т.о. проверки четности бывает достаточно для большинства ситуаций.

Протокол использование контрольных цифр.

В отличие от предыдущего способа для контроля целостности используется не бит, а цифра. Обычно, контролируемый набор цифр вначале по определенным правилам складывается, а затем берется остаток от деления по модулю, который и является контрольной цифрой. Ниже рассматриваются некоторые системы кодирования с использованием контрольной цифры:

- алгоритм Луна;

- штрихкод по стандарту EAN-13;

- заграничный паспорт гражданина РФ с биометрическими данными;

- индивидуальный номер налогоплательщика;

- коды станций на железнодорожном транспорте.

Алгоритм Луна (англ. Luhn algorithm) - алгоритм вычисления контрольной цифры в соответствии со стандартом ISO/IEC 7812 «Идентификационные карты. Идентификация эмитентов». Алгоритм разработан сотрудником фирмы IBM Гансом Питером Луном в 1954 г. Используется для подсчета контрольной цифры:

- номеров всех банковских карт;

- номеров некоторых дисконтных карт;

- кодов полисов обязательного медицинского страхования;

- единого 8-значного номера железнодорожного вагона на РЖД;

- IMEI-кодов (англ. International Mobile Equipment Identity - международный идентификатор мобильного оборудования);

- ICCID-кодов (англ. Integrated Circuit Card ID - идентификатор карты с интегрированной микросхемой);

- т.д.

В следующей таблице приведен порядок вычисления контрольной цифры на примере кода полиса медицинского страхования (рис. 1.2).

Таблица 1

Вычисление контрольной цифры по алгоритму Луна
(если количество цифр в коде четное)

№ п/п	Описание операции	Пример
1	Каждая из цифр, стоящая в нечетной позиции, умножается на 2, после чего вычисляется остаток от деления на 9.	(2 * 2) mod 9 = 4 (5 * 2) mod 9 = 1 (6 * 2) mod 9 = 3 (0 * 2) mod 9 = 0 (4 * 2) mod 9 = 8 (0 * 2) mod 9 = 0 (0 * 2) mod 9 = 0 (1 * 2) mod 9 = 2
2	Вычисляется сумма остатков $\mathbf{S_н}$.	$S_н$ = 4 + 1 + 3 + 0 + 8 + 0 + 0 + 2 = 18

3	Вычисляется сумма цифр $\mathbf{S_ч}$, стоящих в четных позициях, за исключением последней.	$S_ч = 7 + 8 + 2 + 8 + 2 + 0 + 2 = 29$
4	Вычисляется контрольная (последняя) цифра **cd** из уравнения $(S_н + S_ч + cd) \bmod 10 = 0$.	$cd = 3$ $(18 + 29 + 3) \bmod 10 = 0$

Если количество цифр в коде нечетное (например, для IMEI-кодов), то 1 и 2 операция выполняются для цифр, стоящих в четных позициях, 3 операция – для цифр, стоящих в нечетных позициях.

Штрихкод по стандарту EAN-13 - одна из вариаций Европейского стандарта штрихкода, предназначенного для кодирования идентификатора товара и производителя. Регламентируется ГОСТ ИСО/МЭК 15420-2001 «Автоматическая идентификация. Кодирование штриховое. Спецификация символики EAN/UPC (ЕАН/ЮПиСи)».

Рис.1. Штрихкод EAN-13

В следующей таблице приведен порядок вычисления контрольной цифры по стандарту EAN-13.

Таблица 2

№ п/п	Описание операции	Пример
1	Вычисляется сумма цифр $\mathbf{S_н}$, стоящих в нечетных позициях, за исключением последней.	$S_н = 5 + 0 + 2 + 4 + 2 + 4 = 17$
2	Вычисляется утроенная сумма цифр $\mathbf{S_ч}$, стоящих в четных позициях.	$S_ч = 3 * (9 + 1 + 3 + 1 + 3 + 5) = 66$
3	Вычисляется контрольная (последняя) цифра **cd** из уравнения $(S_н + S_ч + cd) \bmod 10 = 0$.	cd = 7 $(17 + 66 + 7) \bmod 10 = 0$

В России с 2009 г. во всех субъектах РФ действуют пункты выдачи паспортно-визовых документов нового поколения - заграничных паспортов гражданина РФ с биометрическими данными.

В документе используются различные способы защиты, в т.ч. защита целостности за счет контрольных цифр. В пластиковой странице с фотографией владельца и встроенным внутри чипом имеется т.н. машиносчитываемая зона (МСЗ).

Рис.3. Машиносчитываемая зона паспорта
(синим контуром выделены контрольные цифры)

В нижней строке МСЗ используются пять контрольных цифр. Ее структура приведена в следующей таблице.

Таблица 3

Структура нижней строки МСЗ

Контрольная цифра	Позиции знака, используемые для расчета контрольных цифр	Позиция контрольной цифры
Номер паспорта	1-9	10
Дата рождения	14-19	20
Дата истечения срока действия паспорта	22-27	28
Личный номер	29-42	43
Заключительная контрольная цифра	1-10, 14-20, 22-43 (позиции 11-13 и 23 исключаются из расчета)	44

Алгоритм расчета контрольных цифр заключается в перемножении каждой цифры соответствующего элемента данных на весовой показатель повторяющейся функции "731 731 ...", суммировании полученных произведений и взятии остатка от деления на 10. Если в элементе данных встречаются буквы латинского алфавита, то при расчете они заменяются на числа от 10 (A) до 35 (Z); знак "<" соответствует 0. Ниже приведен пример расчета контрольных цифр.

Таблица 4

Пример расчета контрольных цифр нижней строки МСЗ

Назначение	Номер паспорта									КЦ				Дата рождения						КЦ		Дата истечения срока действия						КЦ	Личный номер			КЦ	КЦ
№ позиции	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	..	42	43	44
Нижняя строка МСЗ	7	2	5	4	3	6	2	3	9	**5**	R	U	S	7	3	0	1	0	7	**2**	M	2	3	0	7	1	2	**7**	<	...	<	**0**	**2**
Весовой показатель	7	3	1	7	3	1	7	3	1	7				7	3	1	7	3	1	7		7	3	1	7	3	1	7	7	...	3	1	
Расчет контрольной цифры в	(7*7+2*3+5*1+4*7+3*3+6*1+2*7+3*3+9*1) mod 10 = 135 mod 10 = **5**													(7*7+3*3+0*1+1*7+0*3+7*1) mod 10 = 72 mod 10 = **2**								(2*7+3*3+0*1+7*7+1*3+2*1) mod 10 = 77 mod 10 = **7**							(0*7+…+0*3) mod 10 = **0**				

элементеданных											
Расчет заключительной контрольной цифры	[(135 + 5*7) + (72 + 2*7) + (77 + 7*7) + (0 + 0*1)] mod 10 = 382 mod 10 = **2**										

Индивидуальный номер налогоплательщика (ИНН) - уникальный идентификатор, присваиваемый юридическому или физическому лицу для учета уплаты налогов в Российской Федерации. При постановке на налоговый учет подотчетному лицу выдается свидетельство, в котором указывается его ИНН.

Контрольная (контрольные) цифра ИНН определяется по следующим формулам:

- для десятизначного ИНН юридического лица:

$$n_{10} = ((2n_1 + 4n_2 + 10n_3 + 3n_4 + 5n_5 + 9n_6 + 4n_7 + 6n_8 + 8n_9) \bmod 11) \bmod 10; \quad (1)$$

- для двенадцатизначного ИНН физического лица:

$$n_{11} = ((7n_1 + 2n_2 + 4n_3 + 10n_4 + 3n_5 + 5n_6 + 9n_7 + 4n_8 + 6n_9 + 8n_{10}) \bmod 11) \bmod 10, \quad (2)$$

$$n_{12} = ((3n_1 + 7n_2 + 2n_3 + 4n_4 + 10n_5 + 3n_6 + 5n_7 + 9n_8 + 4n_9 + 6n_{10} + 8n_{11}) \bmod 11) \bmod 10, \quad (3)$$

где n_i - i-ая цифра ИНН.

Для ИНН физического лица, отображенного на рис. 4, контрольные цифры:

$$n_{11} = ((7*2 + 2*7 + 4*2 + 10*4 + 3*0 + 5*7 + 9*0 + 4*3 + 6*1 + 8*7) \bmod 11) \bmod 10 = (185 \bmod 11) \bmod 10 = 9 \bmod 10 = 9,$$

$$n_{12} = ((3*2 + 7*7 + 2*2 + 4*4 + 10*0 + 3*7 + 5*0 + 9*3 + 4*1 + 6*7 + 8*9) \bmod 11) \bmod 10 = (241 \bmod 11) \bmod 10 = 10 \bmod 10 = 0.$$

Коды станций на железнодорожном транспорте. В информационных системах железнодорожного транспорта приняты различные способы кодирования станций. В **АСУЖТ** используется код станции, состоящий из 6 цифр ($n_1n_2n_3n_4n_5n_6$). Последняя цифра кода (n_6) является контрольной и определяется по следующей формуле:

$$n_6 = (1n_1 + 2n_2 + 3n_3 + 4n_4 + 5n_5) \bmod 11. \quad (4)$$

Если остаток от деления меньше 10, то он является контрольной цифрой, иначе выполняют сдвиг весового ряда на две позиции и вычисления повторяют:

$$n_6 = (3n_1 + 4n_2 + 5n_3 + 6n_4 + 7n_5) \bmod 11. \quad (5)$$

Если новый остаток от деления вновь получится равным 10, то контрольная цифра принимается равной 0, иначе - остатку, вычисленному по формуле 5.

Первые четыре цифры АСУЖТ для станций, открытых для грузовых операций, называют кодом **Единой сетевой разметки (ЕСР)**. Вариация кода ЕСР с контрольной цифрой состоит из 5 знаков ($n_1n_2n_3n_4n_5$), последний из которых (n_5) определяется точно также, как и для кода станции в АСУЖТ. Отличие заключается в использовании сокращенных весовых рядов (1, 2, 3, 4) и (3, 4, 5, 6). Т.к. пятая цифра для грузовых станций в АСУЖТ принимается равной 0, то контрольные цифры кодов станций АСУЖТ и ЕСР совпадают. В частности, код станции Хабаровск-1 Дальневосточной железной дороги:

- АСУЖТ: код - 970406, контрольная цифра - n_6 = (1*9 + 7*2 + 0*3 + 4*4 + 5*0) mod 11 = 39 mod 11 = 6;

- ЕСР: код - 97046, контрольная цифра - n_5 = (1*9 + 7*2 + 0*3 + 4*4) mod 11 = 39 mod 11 = 6.