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 7. Протоколы контроля целостности. Использование контрольных цифр.

Контрольные суммы (checksums или CRC) являются более надежным способом обеспечения целостности, чем биты четности или контрольные цифры. В англоязычной литературе CRC расшифровывается двояко в зависимости от контекста: Cyclic Redundancy Code или Cyclic Redundancy Check. Под первой расшифровкой понимают циклический код, под второй – хеш-образ.

Циклические коды основаны на полиномиальной арифметике по модулю 2 (полиномиальном делении без переноса). Вместо представления делимого (исходного сообщения, входных данных), делителя (порождающего полинома), частного (целой части) и остатка (контрольной суммы, CRC) в виде положительных целых чисел, их можно представить в виде полиномов с двоичными коэффициентами или в виде строки бит, каждый из которых является коэффициентом полинома. Например, десятичное число 19_{10} в двоичной системе счисления имеет вид 10011_2, что совпадает с полиномом

$$1*x^4 + 0*x^3 + 0*x^2 + 1*x^1 + 1*x^0 = x^4 + x^1 + x^0. \qquad (6)$$

Значение контрольной суммы с порождающим полиномом G(x) определяется по формуле:

$$R(x) = P(x) * x^N \bmod G(x), \qquad (7)$$

где R(x) - полином, представляющий значение контрольной суммы;
P(x) - полином, представляющий входные данные;
G(x) - порождающий полином;
N - максимальная степень порождающего полинома.

Умножение x^N эквивалентно приписыванию N нулевых битов к входным данным. Полиномиальное деление без переноса выполняется по следующим правилам:

- при наличии у промежуточного остатка в качестве старшего бита «1», он складывается по модулю 2 (XOR, исключающее ИЛИ) с битовым представление порождающего полинома и в частное записывается «1»;

- в противном случае выполняется сложение по модулю 2 промежуточного остатка с нулевой битовой строкой длиной N+1 и в частное записывается «0».

В следующей таблице приведены примеры определения контрольных сумм для порождающего полинома $G(x) = x^4 + x^1 + x^0$ (делитель - 10011_2, 19_{10}; N = 4; $x^N = 10000_2$).

Таблица 1

Примеры определения контрольных сумм

Делимое P(x) (входные данные)	10111_2 (23_{10})	10011_2 (19_{10})	10001_2 (17_{10})
$P(x) * x^N$	101110000_2 (368_{10})	100110000_2 (304_{10})	100010000_2 (272_{10})
Деление $P(x) * x^N \bmod G(x)$	101110000 10011 1 01000	100110000 10011 1 00000	100010000 10011 1 00100

	00000 0 10000 10011 1 00110 00000 0 01100 00000 0 1100	00000 0 00000 00000 0 00000 00000 0 00000 00000 0 0000	00000 0 01000 00000 0 10000 10011 1 00110 00000 0 0110
Частное	10100_2 (20_{10})	10000_2 (16_{10})	10010_2 (18_{10})
Остаток R(x) (контрольная сумма)	1100_2 (12_{10})	0000_2 (0_{10})	0110_2 (6_{10})
Входные данные с контрольной суммой	10111 1100_2 (380_{10})	10011 0000_2 (304_{10})	10001 0110_2 (278_{10})

Принимающая сторона для проверки целостности полученных данных может сделать одно из следующих равноценных действий:

- выделить входные данные, вычислить для них контрольную сумму (не забыв при этом дополнить данные N нулевыми битами) и сравнить ее с переданной;

- поделить входные данные с контрольной суммой (последняя строка табл. 2) на делитель, представляющий порождающий полином G(x). В результате должен получиться нулевой остаток.

Как было отмечено выше, использование циклических кодов является более надежным способом контроля целостности, чем биты четности. В то же время, при передаче исходного сообщения P(x) возможна такая его модификация, что контрольная сумма для него и принятого искаженного сообщения P’(x) будут совпадать. Т.е. циклические коды не лишены проблемы возникновения коллизий.

Выбор и применение на практике вида порождающего полинома определяется требованиями производительности и минимизации возникновения коллизий. В следующей таблице приведены некоторые разновидности порождающих полиномов, используемые в информационных системах.

Таблица 2

Разновидности порождающих полиномов

Название	Порождающий полином G(x)	Нормальное представление	Применение
CRC-1	$x + 1$	01_{16}	аппаратный контроль ошибок (нечетный паритетный бит)
CRC-4-ITU	$x^4 + x + 1$	03_{16}	
CRC-7	$x^7 + x^3 + 1$	09_{16}	системы телекоммуникации, MMC, SD
CRC-12	$x^{12} + x^{11} + x^3 + x^2 + x + 1$	$080F_{16}$	системы телекоммуникации
CRC-16-IBM	$x^{16} + x^{15} + x^2 + 1$	8005_{16}	USB, ANSI X3.28
CRC-16-CCITT	$x^{16} + x^{12} + x^5 + 1$	1021_{16}	X.25, Bluetooth, SD, RFID
CRC-24-Radix-64	$x^{24} + x^{23} + x^{18} + x^{17} + x^{14} + x^{11} + x^{10} + x^7 + x^6 + x^5 + x^4 + x^3 + x + 1$	$864CFB_{16}$	OpenPGP
CRC-32-IEEE 802.3	$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$	$1EDC6F41_{16}$	V.42, MPEG-2, PNG
CRC-64-ISO	$x^{64} + x^4 + x^3 + x + 1$	$1B_{16}$	HDLC

Нормальное представление полинома указывается в стандартах, как правило, в шестнадцатеричном виде. При этом преобразование битовой строки полинома выполняется без учета старшего единичного бита.

Например, для CRC-12 битовая строка порождающего полинома выглядит 1100000001111_2. Отбросив старший бит (100000001111_2) и преобразовав в шестнадцатеричный вид, получаем $080F_{16}$.

Другой вариант использования контрольных сумм - проверка целостности хранимых файлов с целью обнаружения их искажения (например, вирусами) или подмены. В этом случае обычно применяют хеш-образы файлов, которые хранятся в защищённом месте и периодически используются для контроля целостности файлов. Хеш-образы активно применяют для проверки целостности скачиваемых файлов. В частности на многих сайтах, помимо дистрибутивов ПО, выкладываются также их контрольные хеш-образы.