



7universum.com  
**UNIVERSUM:**  
**ТЕХНИЧЕСКИЕ НАУКИ**

**UNIVERSUM:**  
**ТЕХНИЧЕСКИЕ НАУКИ**

Научный журнал  
Издается ежемесячно с декабря 2013 года  
Является печатной версией сетевого журнала  
Universum: технические науки

Выпуск: 11(92)

Ноябрь 2021

Часть 1

Москва  
2021

УДК 62/64+66/69

ББК 3

U55

**Главный редактор:**

*Ахметов Сайранбек Махсутович*, д-р техн. наук;

**Заместитель главного редактора:**

*Ахмеднабиев Расул Магомедович*, канд. техн. наук;

**Члены редакционной коллегии:**

*Горбачевский Евгений Викторович*, канд. техн. наук;

*Демин Анатолий Владимирович*, д-р техн. наук;

*Елисеев Дмитрий Викторович*, канд. техн. наук;

*Звезда Марина Юрьевна*, д-р физ.-мат. наук;

*Ким Алексей Юрьевич*, д-р техн. наук;

*Козьминых Владислав Олегович*, д-р хим. наук;

*Ларионов Максим Викторович*, д-р биол. наук;

*Манасян Сергей Керопович*, д-р техн. наук;

*Мажидов Кахрамон Халимович*, д-р наук, проф;

*Мартышкин Алексей Иванович*, канд. техн. наук;

*Мерганов Аваз Мирсултанович*, канд. техн. наук;

*Пайзуллаханов Мухаммад-Султанхан Саидвалиханович*, д-р техн. наук;

*Серегин Андрей Алексеевич*, канд. техн. наук;

*Усманов Хайрулла Сайдуллаевич*, канд. техн. наук;

*Юденков Алексей Витальевич*, д-р физ.-мат. наук;

*Tengiz Magradze*, PhD in Power Engineering and Electrical Engineering.

**U55 Universum: технические науки:** научный журнал. – № 11(92). Часть 1.

М., Изд. «МЦНО», 2021. – 108 с. – Электрон. версия печ. публ. –

<http://7universum.com/ru/tech/archive/category/1192>

ISSN : 2311-5122

DOI: 10.32743/UniTech.2021.92.11-1

Учредитель и издатель: ООО «МЦНО»

ББК 3

© ООО «МЦНО», 2021 г.

## Содержание

<b>Авиационная и ракетно-космическая техника</b>	<b>5</b>
СИСТЕМНЫЙ АНАЛИЗ РАБОТОСПОСОБНОСТИ ЭНЕРГОУСТАНОВКИ СРЕДНЕЙ МОЩНОСТИ Булгаков Артем Евгеньевич Шавлов Алексей Валерьевич	5
ИСПОЛЬЗОВАНИЕ МЕТОДА МОНТЕ-КАРЛО ДЛЯ ОБНАРУЖЕНИЯ ТРАЕКТОРИИ ПРОТИВОРАДИОЛОКАЦИОННОЙ РАКЕТЫ, НАВОДЯЩЕЙСЯ НА РАДИОЛОКАЦИОННОЙ СТАНЦИИ ОБЗОРА Мухаммедов Бобомурод Мухаммадкаримович Норкулов Элиёр Облакулович	8
РАДИОЛОКАЦИОННАЯ СИСТЕМА ПОСАДКИ РСР-6М2 КАК ОБЪЕКТ ПОРАЖЕНИЯ ПРОТИВОРАДИОЛОКАЦИОННЫМИ РАКЕТАМИ Хуррамов Жамшид Ахрорович	14
ВНЕДРЕНИЕ ПРИМЕНЕНИЯ ЭЛЕКТРОННОГО ПОЛЕТНОГО ПЛАНШЕТА В БОЕВОЙ АВИАЦИИ НА ЭТАПАХ ПОДГОТОВКИ И ВЫПОЛНЕНИЯ ПОЛЕТНОГО ЗАДАНИЯ Шевелёв Антон Анатольевич	20
<b>Безопасность деятельности человека</b>	<b>25</b>
ХАРАКТЕРИСТИКА ВОЗДЕЙСТВИЯ МИНИ – ЦЕХА КОНСЕРВАЦИИ НА ОКРУЖАЮЩУЮ СРЕДУ Домуладжанов Ибрагимжон Хаджимухамедович Домуладжанова Шахло Ибрагимовна Латипова Мухайё Ибрагимжановна Махмудов Содир Юсуфалиевич	25
ИНФОРМАЦИОННО - КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ В УСЛОВИЯХ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ Тилавалдиев Бахтияр Тилавалдиевич Абдуллаев Зокиржон Джураевич	31
<b>Инженерная геометрия и компьютерная графика</b>	<b>34</b>
ТРАДИЦИОННЫЕ И АДДИТИВНЫЕ ТЕХНОЛОГИИ В ПРОИЗВОДСТВЕ ДЕТАЛЕЙ МАШИН Ахмедова Шахноза Асаджановна	34
ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ВЫПОЛНЕНИИ ГРАФИЧЕСКИХ РАБОТ Умарова Дильфуза Сатволдиевна	38
<b>Информатика, вычислительная техника и управление</b>	<b>41</b>
ВАЖНЫЕ ФУНКЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ CRM Атабаева Элиза Руслановна Моисеенко Наталья Анатольевна	41
ИССЛЕДОВАНИЕ И ВНЕДРЕНИЕ СИСТЕМЫ МОНИТОРИНГА ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ Дакуева Элина Рамзановна Мачуева Дина Алуевна	44
ПРОЦЕДУРЫ ОПТИМИЗАЦИИ ГЛОБАЛЬНЫХ ЦЕЛЕЙ СИСТЕМЫ УПРАВЛЕНИЯ МНОГОСТАДИЙНЫМИ ПРОЦЕССАМИ Каримов Жасурбек Хасанбоевич	48
ПРИМЕНИМОСТЬ ЭНЕРГОЭФФЕКТИВНЫХ, ЭНЕРГОСБЕРЕГАЮЩИХ ТЕХНОЛОГИЙ И ТЕХНОЛОГИЙ SMART HOME, IOT ПРИ СТРОИТЕЛЬСТВЕ ЧАСТНЫХ ЖИЛЫХ ОБЪЕКТОВ В ЮЖНОЙ ЧАСТИ ПРИМОРСКОГО КРАЯ Лепинских Александр Николаевич Поддубный Иван Владиславович Рузин Максим Евгеньевич Кравцов Данила Станиславович Федоров Дмитрий Алексеевич	53
РАСПОЗНАВАНИЕ ЖЕСТОВ РУК С ПОМОЩЬЮ MobileNetV2 Махмудов Миршод Дилшод угли Фазилова Дилбархон Шамурадовна	60

РАЗВИТИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СИСТЕМЕ ОБРАЗОВАНИЯ	63
Межиева Белкист Усмановна	
Моисеенко Наталья Анатольевна	
АЛГОРИТМЫ ШИФРОВАНИЯ И ИХ СВОЙСТВА	66
Тахиров Бехзод Насриддинович	
<b>Машиностроение и машиноведение</b>	<b>69</b>
О ВОПРОСАХ ПОВЫШЕНИЯ ДОЛГОВЕЧНОСТИ КОЛЕНЧАТЫХ ВАЛОВ ГРУЗОВЫХ АВТОМОБИЛЕЙ БОЛЬШОЙ МОЩНОСТИ	69
Аллаяров Тимур Азатович	
Суннатов Ихтиер Хикматович	
Мирнигматов Шукурулло Ботир угли	
ТЕХНОЛОГИЧЕСКИЙ РАСЧЕТ СТАНЦИЙ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ, С УЧЕТОМ ЧИСЛО ЗАЕЗДОВ И КОЛИЧЕСТВО ОБСЛУЖИВАЕМЫХ АВТОМОБИЛЕЙ	72
Кадиршаев Тургунбай	
Ибрахимов Каримжан Исмаилович	
УСЛОВИЯ ПЛАСТИЧНОСТИ	76
Махмудова Наргиза Абдунабиевна	
РАЗРАБОТКА СПОСОБА ИЗМЕЛЬЧЕНИЯ СТЕБЛЕЙ ХЛОПЧАТНИКА ДЛЯ ПОЛУЧЕНИЯ КОНДИЦИОННОЙ ДРЕВЕСНОВОЛОКНИСТОЙ МАССЫ ДЛЯ ПРОИЗВОДСТВА ДРЕВЕСНО-ПЛАСТИКОВЫХ ПЛИТ	80
Негматов Сайибжан Садикович	
Мадрахимов Аллоберди Махмадалиевич	
Абед Нодира Сойибжановна	
Негматова Комила Сайибжановна	
Бойдадаев Мурод Бойдада угли,	
Холмуродова Дилафруз Куватовна	
Жалилов Шерали Некбоевич	
ИССЛЕДОВАНИЕ МЕХАНИЧЕСКОЙ ПРОЧНОСТИ ДВИГАТЕЛЯ ТИПА СПД-50	87
Ольшанская Ольга Викторовна	
Ярисов Владимир Владимирович	
РАЗРАБОТКА И ИССЛЕДОВАНИЕ СПОСОБА АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ ПРОЦЕССОМ НАМАТЫВАНИЯ РОВНИЦЫ И КРУТИЛЬНО-МОТАЛЬНОГО МЕХАНИЗМА РОВНИЧНОЙ МАШИНЫ	95
Соркин Аркадий Павлович	
Бабаджанов Собит Хусанович	
Джурабекова Нодира Рахимбековна	
Касимов Аброр Алиёрович	

## АЛГОРИТМЫ ШИФРОВАНИЯ И ИХ СВОЙСТВА

*Тахиров Бехзод Насриддинович*

*преподаватель,  
Бухарский государственный университет,  
Республика Узбекистан, г. Бухара  
E-mail: [evrikiy@list.ru](mailto:evrikiy@list.ru)*

## ENCRYPTION ALGORITHMS AND THEIR PROPERTIES

*Behzod Takhirov*

*Lecturer, Bukhara State University,  
Republic of Uzbekistan, Bukhara*

### АННОТАЦИЯ

Проблемой защиты информации человечество занимается с момента появления письменности. Эта проблема возникла из-за необходимости тайно передавать военную и дипломатическую информацию. Например, древние спартанцы зашифровывали военную информацию. Описание китайцами простой письменности в виде иероглифов позволило скрыть ее от иностранцев.

### ABSTRACT

Humanity has been dealing with the problem of information protection since the advent of writing. This problem arose because of the need to secretly transmit military and diplomatic information. For example, the ancient Spartans encrypted military information. The Chinese description of simple writing in the form of hieroglyphs made it possible to hide it from foreigners.

**Ключевые слова:** криптография, шифрование, дешифрование, код, ключ.

**Keywords:** cryptography, encryption, decryption, code, key.

Термин «криптография» в переводе с греческого означает скрывать запись. Значение термина означает, что криптография применяется с целью скрытого хранения и защиты необходимой информации.

XX век до нашей эры. Во время раскопок в Месопотамии были обнаружены древнейшие зашифрованные тексты. Текст, начертанный колышками на глиняной доске, был рецептом краски, которую мастера изготавливали для покрытия керамических изделий, что считалось коммерческой тайной. Также известны религиозные надписи и медицинские рецепты древних египтян.

Середина девятого века до нашей эры. Согласно Плутарху, именно в этот период было применено шифровальное устройство – scital, которое позволяло шифровать текст с помощью подстановок. При расшифровке текста слова записывались на узкую ленту, завернутую в цилиндр (косу) определенного диаметра. Когда лента растекалась, на ней образовывалась позиция, в которой буквы открытого текста заменялись местами. Ключом в этом служил диаметр цилиндра. Способ расшифровки такого текста был предложен Аристотелем. Он наматывал ленту на конус и посчитал, что диаметр цилиндра - это место, которое указывает на слово или часть слова, которое можно прочитать.

56 год нашей эры. У.Цезарь использовал заменяющий тип шифра во время войны с галлами. Этот алфавит был написан путем перемещения по циклу (на три позиции в Цезаре) под алфавитом открытого

текста. При шифровании алфавиты в открытом тексте, то есть буквы, расположенные сверху, заменяются соответствующими буквами внизу. Этот тип шифрования был известен еще до Цезаря, но такой способ шифрования носит его имя.

К традиционным (классическим) методам шифрования относятся шифры замен, шифры простых и сложных замен и их комбинации и модификации. Следует отметить, что комбинации шифров замещения и шифров замещения составляют различные виды симметричных шифров, которые используются на практике.

В шифрах замещения буквы шифруемого текста заменяются по определенным правилам внутри этого блока текста. Шифры замещения являются самыми простыми и древними.

*Шифровальные таблицы.* В начале эпохи Возрождения (конец XIV в.) в шифрах замен использовались шифровальные таблицы. В качестве ключа к шифровальным таблицам выступают: размер таблицы; слово или предложение, определяющие замену; которые являются особенностью структуры таблицы.

Самым простым является табличное шифрование, когда в качестве ключа задается размер таблицы. Пусть дан следующий текст:

### ОБЪЕКТ BELGILANGAN JOYGA BORADI

Эта информация вносится в таблицу последовательно по столбцам:

O	K	L	A	N	G	R
B	T	G	N	J	A	A
Y	B	I	G	O	B	D
E	E	L	A	Y	O	I

В результате формируется таблица размером 4x7. Теперь зашифрованный текст определяется по строкам, то есть мы пишем его, выделяя для себя 4 символа.

**OKLA NGRB TGNJ AAУВ IGOB DEEL AYOI**

Ключевым моментом здесь служат размеры таблицы. Естественно, источник и получатель должны договориться между собой о том, что ключ должен соответствовать размерам таблицы. При расшифровке выполняется обратное действие.

*Шифрование с помощью простой замены*

Буквы шифруемого текста заменяются буквами того или иного алфавита по заданной схеме. В шифре простой замены каждая буква заданного текста заменяется другой соответствующей ей буквой в том же алфавите. Обычно такой способ шифрования называют шифром однобуквенной замены.

*Система шифрования Цезаря.* Метод шифрования Цезаря является частным случаем простого шифра замены. В этом методе каждая буква алфавита заменяется на букву, которая стоит на месте сдвига на число K, которая умножается на число. При достижении конца алфавита, сдвиг начинается с его начала. Цезарь использовал сдвиг, который был равен трём, т.е. K=3. В таблице ниже приведено соответствие букв латинского алфавита сдвигу равному трём:

0	1	2	3	4	5					10					15					20					25
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
					<b>D</b>	<b>I</b>	<b>P</b>	<b>L</b>	<b>O</b>	<b>M</b>	<b>A</b>	<b>T</b>													

Пишется после ключевого слова в остальной алфавитной последовательности.

0	1	2	3	4	5					10					15					20					25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
V	W	X	Y	Z	<b>D</b>	<b>I</b>	<b>P</b>	<b>L</b>	<b>O</b>	<b>M</b>	<b>A</b>	<b>T</b>	V	C	E	F	G	H	J	K	N	Q	R	S	U

В результате определяются буквы-заменители, соответствующие буквам данного текста. Если открытый текст выглядит как TOVAR KELDI, то после шифрования преобразуется в текст JCNVG MZAYL.

*Система шифрования Вижинера.* Система шифрования, созданная французским дипломатом XVI века Вижинером, была опубликована в 1586 году. Она считается популярной многоалфавитной системой. Система Вижинера считается более совершенной, чем система шифрования Цезаря, в которой ключ заменяется с буквы на букву. Такой шифр многоалфавитной замены можно представить через шифровальную таблицу. В приведенных ниже таблицах приведены соответствующие таблицы для русского

A	D	J	M	S	V
B	E	K	N	T	W
C	F	L	O	U	X
D	G	M	P	V	Y
E	H	N	Q	W	Z
F	I	O	R	X	A
G	J	P	S	Y	B
H	K	Q	T	Z	C
I	L	R	U		

Сообщение Цезаря «Пришел, увидел, победил» содержание VENI VIDI

VICI, принимает следующий вид YHQL YLGL YLFL, когда предложение шифруется предложенным им способом.

Недостатком метода Цезаря является то, что одни и те же буквы чередуются, в свою очередь, на одни и те же буквы. Используя частоту повторения букв в криптосистеме, зашифрованный таким образом текст можно быстро расшифровать.

*Ключевые слова системы Цезарь.* Система Цезаря шифрования ключевыми словами представляет собой систему однобуквенных замен. В этом методе используется перелистывание и изменение порядка букв по ключевому слову.

Давайте возьмем слово DIPLOMAT в качестве ключевого слова и сдвиг равный пяти. Ключевое слово пишется под алфавитом, сдвинутым на пять букв:

и латинского алфавитов. Это текст из таблиц он используется для шифрования и дешифрования.

– Буквы в верхнем ряду используются для входящего открытого письма.

– в левом столбце будет размещено ключевое слово.

При шифровании открытого текста этот текст записывается в одну строку. Ключевое слово помещается в строку под ним. Если длина ключевого слова короткая, это слово повторяется до последней буквы открытого текста. В процессе шифрования обнаруживается буква открытого текста, находящаяся в верхней части таблицы, а из левой части выбирается буква ключевого слова. Буква ячейки, в которой пересекаются строка и столбец, заменяет заданную букву.

Послание	B	A	Y	R	A	M	K	U	N	I
Ключ	V	A	Z	A	V	A	Z	A	V	A
Зашифрованный текст	G	A	R	R	V	M	S	U	P	I

		PLAINTEXT LETTERS																									
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
KEYWORD LETTERS	A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Таким образом, мы рассмотрели способы шифрования, которые используются для обучения студентов шифрованию во время занятий по компьютерной безопасности.

**Список литературы:**

1. Бабаш А.В. История криптографии. Часть I - М.: Гелиос АРВ, 2016. - 240 с.
2. Тахиров Б.Н. Понятие виртуальной реальности // Наука, образование и культура. 2014. № 1 (1). С. 12-14.
3. Хаятов Х.У., Тахиров Б.Н. Постановка обратной задачи для уравнений математической физики // Academy, № 10 (61), 2020. С.32-35.
4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си - М.: Триумф, 2012. - 518 с.
5. Зарипова Г.К., Сайидова Н.С., Тахиров Б.Н., Хайитов У.Х. Педагогическое сотрудничество преподавателя и студентов в кредитно-модульной системе высшего образования // Наука, образование и культура, № 8 (52), 2020. С. 22-26.