

А. В. ЗЕНКОВ

# ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

		O	P	Q	R	S	T	V	X	A	B	C	D	E	F	G	H	I	L	M	N
		<i>E</i>	<i>I</i>	<i>G</i>	<i>H</i>	<i>I</i>	<i>L</i>	<i>M</i>	<i>N</i>	<i>O</i>	<i>P</i>	<i>Q</i>	<i>R</i>	<i>S</i>	<i>T</i>	<i>V</i>	<i>X</i>	<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>
O	<i>E</i>	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	f	t	v	x
P	<i>F</i>	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	f	t	v	x	a
Q	<i>G</i>	e	d	c	f	g	h	i	l	m	n	o	p	q	r	f	t	v	x	a	b
R	<i>H</i>	d	e	f	g	h	i	l	m	n	o	p	q	r	f	t	v	x	a	b	c
S	<i>I</i>	c	f	g	h	i	l	m	n	o	p	q	r	f	t	v	x	a	b	c	d
T	<i>L</i>	f	g	h	i	l	m	n	o	p	q	r	f	t	v	x	a	b	c	d	e
V	<i>M</i>	g	h	i	l	m	n	o	p	q	r	f	t	v	x	a	b	c	d	e	f
X	<i>N</i>	h	i	l	m	n	o	p	q	r	f	t	v	x	a	b	c	d	e	f	g
A	<i>O</i>	i	l	m	n	o	p	q	r	f	t	v	x	a	b	c	d	e	f	g	h
B	<i>P</i>	l	m	n	o	p	q	r	f	t	v	x	a	b	c	d	e	f	g	h	i
C	<i>Q</i>	m	n	o	p	q	r	f	t	v	x	a	b	c	d	e	f	g	h	i	l
D	<i>R</i>	n	o	p	q	r	f	t	v	x	a	b	c	d	e	f	g	h	i	l	m
E	<i>S</i>	o	p	q	r	f	t	v	x	a	b	c	d	e	f	g	h	i	l	m	n
F	<i>T</i>	p	q	r	f	t	v	x	a	b	c	d	e	f	g	h	i	l	m	n	o
G	<i>V</i>	q	r	f	t	v	x	a	b	c	d	e	f	g	h	i	l	m	n	o	p
H	<i>X</i>	r	f	t	v	x	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q
I	<i>A</i>	f	t	v	x	a	b	c	d	e	f	g	h	i	l	n	n	o	p	q	r
L	<i>B</i>	t	v	x	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	f
M	<i>C</i>	v	x	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	f	t
N	<i>D</i>	x	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	f	t	v

**А. В. ЗЕНКОВ**

# **ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Учебное пособие

Москва Вологда  
«Инфра-Инженерия»  
2022

УДК 681.3.06  
ББК 32.973  
3-56

Рецензенты:

доктор педагогических наук, профессор кафедры информационных технологий и статистики Уральского государственного экономического университета *Плещёв Владимир Васильевич*;  
кандидат физико-математических наук, доцент кафедры шахматного искусства и компьютерной математики Уральского государственного экономического университета *Мельников Юрий Борисович*

**Зенков, А. В.**

**3-56** Основы информационной безопасности : учебное пособие / А. В. Зенков. – Москва ; Вологда : Инфра-Инженерия, 2022. – 104 с. : ил., табл.  
ISBN 978-5-9729-0864-6

Даны базовые понятия, связанные с информационной безопасностью и защитой информации. Изложены математические основы некоторых криптографических алгоритмов. Включены упражнения, материалы для проведения практических занятий и постановка задач для лабораторных работ.

Для студентов IT-специальностей по направлениям «Бизнес-информатика», «Информатика и вычислительная техника», «Фундаментальная информатика и информационные технологии».

УДК 681.3.06  
ББК 32.973

На обложке приведена таблица Виженера (для латинского алфавита) в том виде, в котором она была опубликована в знаменитом трактате «Traicté des Chiffres ou Secrètes Manières d'Escrire» Блеза де Виженера (1586 г.). Шифр Виженера является классическим представителем симметричных шифров и подробно рассматривается в настоящем учебном пособии. Трактат Виженера находится в открытом доступе по адресу <https://gallica.bnf.fr/ark:/12148/bpt6k73371g.image>

ISBN 978-5-9729-0864-6

© Зенков А. В., 2022  
© Издательство «Инфра-Инженерия», 2022  
© Оформление. Издательство «Инфра-Инженерия», 2022

## ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ.....	3
ГЛАВА 1. ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ.....	5
ГЛАВА 2. ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ.....	9
ГЛАВА 3. КРИПТОГРАФИЯ.....	26
ГЛАВА 4. МАТЕРИАЛЫ К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ: ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ.....	60
ГЛАВА 5. УСЛОВИЯ ЛАБОРАТОРНЫХ РАБОТ.....	90
ПРИЛОЖЕНИЕ.....	92
ЛИТЕРАТУРА.....	95
ТЕСТЫ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЕ ИНФОРМАЦИИ.....	96