

Индекс 79187

ISSN 2073-2600

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

3

(142)

*Подписывайтесь,
читайте,*

пишите в наш журнал

Москва 2023



Все новейшие достижения и современные разработки предприятий оборонного комплекса — в научно-технических журналах ФГУП «НТЦ оборонного комплекса «Компас»

ФГУП «Научно-технический центр оборонного комплекса «Компас» является издателем следующих научных журналов:



Межотраслевой научно-технический журнал
Оборонный комплекс — научно-техническому прогрессу России
(4 выпуска)
Подписной индекс **79379**
Издается с 1984 года



Межотраслевой научно-технический журнал
Конструкции из композиционных материалов
(4 выпуска)
Подписной индекс **80089**
Издается с 1981 года



Научно-технический журнал
Информационные технологии в проектировании и производстве
(4 выпуска)
Подписной индекс **79378**
Издается с 1976 года



Межотраслевой научно-практический журнал
Экология промышленного производства
(4 выпуска)
Подписной индекс **80090**
Издается с 1993 года



Научно-практический журнал
Вопросы защиты информации
(4 выпуска)
Подписной индекс **79187**
Издается с 1974 года

Все издания ФГУП «Научно-технический центр оборонного комплекса «Компас»:

✓ включены решением ВАК Министерства науки и высшего образования России в перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени кандидата и доктора наук;

✓ метаданные выпусков включены в базу данных Российского индекса научного цитирования (РИНЦ).

Более подробную информацию об изданиях, подписке, дополнительных услугах можно получить по тел.: 8 (495) 491-43-17, 8 (495) 491-77-67, 8 (495) 491-77-20 (подписка);
факс: 8 (495) 491-44-80.
E-mail: izdanie@ntckompas.ru

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

3
(142)

Москва
2023

Основан
в 1974 г.

СОДЕРЖАНИЕ

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Инженерная криптография

Симон А. Б. Новое о шифре Уитстона (продолжение) 3

Доверенная среда

Былевский П. Г., Возможности и ограничения цифровой динамической биометрической идентификации 12

Васильев Р. А., Ляхманов Д. А., Капранов С. Н. Разработка метода генерации речеподобной помехи с применением фонов идентифицированного по голосу диктора 18

Иниватов Д. П. Аналитическое исследование проблемы биометрической идентификации и аутентификации субъектов по голосу 28

ОБЩИЕ ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ОБЪЕКТОВ

Лапсарь А. П., Любухин А. С. Выбор оптимальной по точности контрольной аппаратуры для оценки эффективности защиты информации 39

Кабаков В. В. Обеспечение информационной безопасности предприятия на основе риск-ориентированного подхода к проведению аудита информационной безопасности 46

Сидорин С. Ю., Благовещенский И. Г., Соболева Е. А., Шармаев В. И. Киберустойчивость предприятий пищевой промышленности: определение потенциальных векторов атаки 51

Недбайло Ю. А., Сурченко А. В., Пиков В. А. Алгоритм интерливинга распределённого общего кэша многоядерного процессора для произвольного количества банков 59

Главный редактор **В. Г. Матюхин**,
д-р техн. наук, первый заместитель генерального
директора, научный руководитель ОАО "НИИАС"

Заместитель главного редактора **В. А. Коняевский**,
д-р техн. наук, зав. кафедрой МФТИ

Ответственный секретарь **К. В. Трыкина**,
начальник отдела научных и информационных
изданий ФГУП «НТЦ оборонного комплекса
«Компас»

Редакционная коллегия:

М. М. Грунтович, канд. физ.-мат. наук, доц., руководитель обособленного подразделения АО "Инфотекс"; **С. В. Дворянкин**, д-р техн. наук, проф., профессор кафедры Финансового университета; **С. М. Климов**, д-р техн. наук, проф., начальник управления 4 ЦНИИ МО; **В. П. Лось**, д-р воен. наук, проф., зав. кафедрой МТУ; **И. Г. Назаров**, канд. техн. наук, генеральный директор ОКБ САПР; **С. П. Панасенко**, канд. техн. наук, директор по научной работе компании «Актив»; **Г. В. Росс**, д-р техн. наук, д-р эконом. наук, проф., главный научный сотрудник лаборатории семантического анализа и интеграции Российского экономического университета им. Г. В. Плеханова; **В. Ю. Скиба**, д-р техн. наук, первый зам. начальника Главного управления информационных технологий ФТС России; **А. А. Стрельцов**, д-р техн. наук, д-р юр. наук, проф., зам. директора Института проблем информационной безопасности МГУ им. М. В. Ломоносова; **А. М. Сычёв**, д-р техн. наук, первый заместитель директора департамента информационной безопасности Банка России; **Ю. С. Харин**, д-р физ.-мат. наук, чл.-кор. НАН Беларуси, директор НИИ прикладных проблем математики и информатики БГУ; **И. Б. Шубинский**, д-р техн. наук, проф., генеральный директор ЗАО "ИБТранс", советник генерального директора ОАО "НИИАС"; **Ю. К. Язов**, д-р техн. наук, проф., главный научный сотрудник управления ГНИИИ ПТЗИ ФСТЭК России.

Вопросы защиты информации: Науч.-практ. журн. / ФГУП «НТЦ оборонного комплекса «Компас», 2023.
Вып. 3 (142). С. 1—68.

Компьютерная верстка: *Н. В. Ильина, К. В. Трыкина*

Подписано в печать 14.09.2023. Формат 60x84 1/8.
Печать офсетная. Усл. печ. л. 7,0 . Уч.-изд. л. 7, 2.
Тираж 400 экз. Заказ 2022. Свободная цена.
Адрес редакции: 125424, Москва,
Волоколамское ш., 77. ФГУП «НТЦ оборонного комплекса «Компас».
<http://ntckompas.ru>
Отпечатано: 101000, Москва,
Лубянский проезд, д. 15, стр. 4, офис 105.
ИП Кириченко Алексей Викторович.
Индекс 79187.

ИНЖЕНЕРНАЯ КРИПТОГРАФИЯ

УДК 681.3.06

DOI: 10.52190/2073-2600_2023_3_3

EDN: RJFJGQ

Новое о шифре Уитстона (продолжение)

А. Б. Симон

ПАО «Уралмашзавод», г. Екатеринбург, Россия

Описан алгоритм симметричного блочного шифрования на базе контекстной замены знаков текста. Шифр допускает параллельные вычисления на уровне блоков и обеспечивает высокую скорость шифрования. Даны примеры однораундного шифрования при достаточном уровне криптостойкости.

Ключевые слова: контекст, замена, массив, пара, знак, однораундный, многопоточный.

В [1] описано шести- и восьмираундное шифрование в нестандартных режимах на основе замен знаков по Уитстону. Для сравнения покажем результаты одного раунда шифрования в стандартных режимах OFB, CBC и CFB [2]. Опишем порядок многопоточного шифрования в этих же режимах.

Базовый пример одного раунда шифрования

Напомним правила замен и дадим пример одного раунда шифрования (табл. 1).

Таблица 1

Один раунд шифра контекстной замены знаков текста

Шаг	Сдвиг Δ	Шифрующие массивы	Текст
1	0	$A_0 - A_R$	до замены
			после замены
2	1	$A_1 - A_R$	до замены
			после замены
3	2	$A_2 - A_R$	до замены
			после замены
4	3	$A_3 - A_R$	до замены
			после замены

Примечание. Заменяемые и заменяющие знаки подчеркнуты. За один раунд открытый текст 05a7 заменён на шифртекст f5c3.

Симон Адольф Брунович, ведущий конструктор.
E-mail: simonadol@yandex.ru

Статья поступила в редакцию 10 мая 2023 г.

© Симон А. Б., 2023

Возьмём расширенный ключ из массивов A_0 и A_R (рис. 1).

A_0	A_1	A_2	A_3	A_R
0 1 2 3	4 5 6 7	8 9 a b	c d e f	6 a c d
4 5 6 7	8 9 a b	c d e f	0 1 2 3	7 e 0 8
8 9 a b	c d e f	0 1 2 3	4 5 6 7	5 b 1 f
c d e f	0 1 2 3	4 5 6 7	8 9 a b	3 2 9 4

Рис. 1. Шифрующие массивы

Поочерёдным сдвигом массива A_0 относительно массива A_R на одну строку вверх получим дополнительные шифрующие массивы A_1 , A_2 и A_3 . Величину сдвига на каждом шаге шифрования в табл. 1 показывает параметр $\Delta = 0, 1, 2, 3$.

Перечислим правила контекстной замены знаков текста.

- Пара массивов выполняет замену пары знаков текста. В зависимости от алфавита, используемого в шифре, знаки могут иметь размер 4, 6 или 8 бит. Например, в шифре с массивами 16×16 использован байтовый алфавит со знаками 8 бит, в шифре с массивами 8×8 — алфавит со знаками 6 бит. Данные правила подходят для замены знаков всех указанных размеров.

- Каждая пара знаков смещается относительно предыдущей на один знак вправо (подчёркнутые пары в табл. 1). Одновременно меняется и шифрующая пара массивов. Смещение только на одну позицию обеспечивает контекстность замен, когда на замену данного знака прямо или косвенно влияют предыдущие знаки и один следующий.

- Заменяющий знак берут из того же массива, в котором находится заменяемый. Например, если

знак находится в массиве A_1 , замену ему надо брать тоже в массиве A_1 .

- Левый знак пары находят в левом массиве, правый — в правом. Эти знаки считают углами воображаемого прямоугольника и в других углах берут замену. Например, знак 0 из шага 1 табл. 1 находим в массиве A_0 , знак 5 — в массиве A_R , считаем эти знаки углами прямоугольника и в других углах берём замену 86.

- Если оба знака находятся в одной строке, левый заменяющий знак заимствует координаты правого заменяемого знака, а правый заменяющий знак — левого заменяемого знака. Например, знаки ба из шага 2 будут заменены на 5с.

- Если у заменяемых знаков одинаковые координаты, замены не производят (шаг 3).

- В паре "последний знак блока—первый знак блока" последний знак блока заменяют в левом массиве, первый — в правом. Например, в шаге 4 знак 7 заменяют на 3 в массиве A_3 , а знак 8 — на f в массиве A_R . Шаг 4 кольцует замены знаков в границах блока. Это обеспечивает сплошную, кольцевую, контекстную взаимозависимость знаков друг от друга.

Пример шифрования в режиме OFB

В этом режиме возможно шифрование в два этапа (рис. 2).

Этап 1 — создание блоков гаммы. Первый блок получают контекстной заменой знаков синхропосылки. Следующие блоки — заменой знаков гаммы предыдущего блока. На этом этапе можно подготовить гамму нужного размера до получения открытого текста.

Этап 2 — потоковое создание шифртекста. Гамма и открытый текст побитно суммируются по модулю 2.

Начальные условия шифрования:

- ключевые массивы — V_0 (табл. 2) и V_R (табл. 3);
- размер блока — 128 бит;
- синхропосылка — 0000 0000 0000 0000 0000 0000 0000;
- открытый текст у всех блоков — 0000 0000 0000 0000 0000 0000 0000;
- очередь сдвигов Δ — 0123456789abcdef;
- число раундов — один.

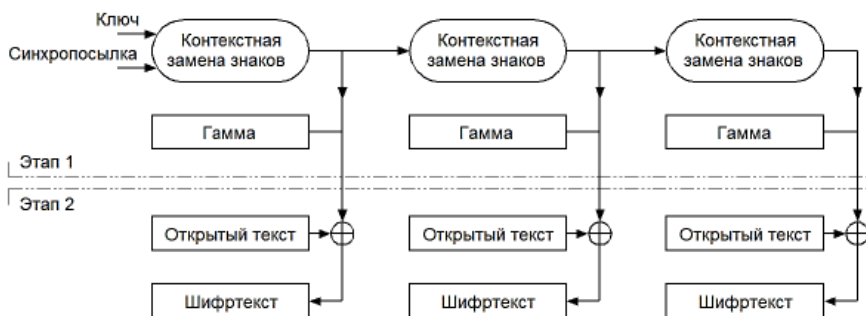


Рис. 2. Режим гаммирования с обратной связью по выводу OFB

Таблица 2

Ключевой массив левый V_0 (байты размещены по возрастанию)

f	0f	1f	2f	3f	4f	5f	6f	7f	8f	9f	af	bf	cf	df	ef	ff
e	0e	1e	2e	3e	4e	5e	6e	7e	8e	9e	ae	be	ce	de	ee	fe
d	0d	1d	2d	3d	4d	5d	6d	7d	8d	9d	ad	bd	cd	dd	ed	fd
c	0c	1c	2c	3c	4c	5c	6c	7c	8c	9c	ac	bc	cc	dc	ec	fc
b	0b	1b	2b	3b	4b	5b	6b	7b	8b	9b	ab	bb	cb	db	eb	fb
a	0a	1a	2a	3a	4a	5a	6a	7a	8a	9a	aa	ba	ca	da	ea	fa
9	09	19	29	39	49	59	69	79	89	99	a9	b9	c9	d9	e9	f9
8	08	18	28	38	48	58	68	78	88	98	a8	b8	c8	d8	e8	f8
7	07	17	27	37	47	57	67	77	87	97	a7	b7	c7	d7	e7	f7
6	06	16	26	36	46	56	66	76	86	96	a6	b6	c6	d6	e6	f6
5	05	15	25	35	45	55	65	75	85	95	a5	b5	c5	d5	e5	f5
4	04	14	24	34	44	54	64	74	84	94	a4	b4	c4	d4	e4	f4
3	03	13	23	33	43	53	63	73	83	93	a3	b3	c3	d3	e3	f3
2	02	12	22	32	42	52	62	72	82	92	a2	b2	c2	d2	e2	f2
1	01	11	21	31	41	51	61	71	81	91	a1	b1	c1	d1	e1	f1
0	00	10	20	30	40	50	60	70	80	90	a0	b0	c0	d0	e0	f0
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f

Таблица 3

Ключевой массив правый V_R (байты размещены хаотично)

f	84	41	7e	79	de	6f	a5	08	30	e5	4f	da	8b	ba	44	3b
e	f7	67	2c	23	ef	c4	d2	85	1c	f0	86	f9	b0	33	5c	57
d	af	34	5a	4b	3d	4c	21	dc	8f	a8	12	6d	7b	0c	2e	a0
c	ad	37	02	54	d1	89	69	51	78	b5	c8	59	55	47	73	0a
b	cd	7f	c5	f6	93	28	1b	16	f4	7c	96	0f	bc	f1	f3	95
a	a7	0b	d5	40	17	43	ce	39	b9	6b	8d	72	fd	70	3c	49
9	4e	7a	56	ec	29	cc	99	c6	b8	07	d0	2d	19	d6	76	27
8	68	3e	15	24	53	f2	05	b7	9b	e9	5b	97	a1	38	01	32
7	9f	aa	3f	1a	ed	35	26	e2	11	b1	8c	a3	1e	90	b6	a4
6	64	b2	ea	e6	c2	fa	ae	c0	62	36	81	1d	04	42	65	cb
5	ac	cf	e1	0e	7d	94	e0	13	fb	e4	48	fe	4a	74	9d	db
4	3a	82	50	2b	31	ee	ca	bf	9e	75	00	61	d3	6c	ff	45
3	1f	5f	20	c1	f5	03	c7	a9	d7	d8	c9	58	e3	5e	46	2a
2	09	2f	fc	98	d9	e7	b3	e8	a6	dd	77	8a	f8	22	63	8e
1	5d	91	88	60	0d	c3	bd	18	b4	bb	92	d4	83	9c	87	10
0	be	25	06	df	eb	6a	6e	ab	9a	71	66	14	80	a2	52	4d
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f

В табл. 4 даны результаты первого этапа шифрования, т. е. показаны шесть блоков однораундной гаммы. Если эти блоки побитно сложить по модулю 2 с каким-нибудь открытым текстом, получим шифртекст из шести блоков по 128 бит. При смене синхропосылки сменятся гамма и шифртекст. Так как в нашем случае открытый текст у всех блоков 00...00, результаты первого и второго этапов совпадают. Дополнительные пары массивов создавались поочерёдным сдвигом массива V_0 относительно массива V_R на одну строку вверх.

В табл. 5 показана пошаговая зашифровка блока 1 табл. 4. Для каждой процедуры замены знаков (в данном случае заменяются байты) дана пара шифрующих массивов. Например, массивы V_2 — V_R заменяют байты 8c и 00 на 82 и 86. Массив V_2 получен сдвигом массива V_0 на две строки вверх ($\Delta = 2$) относительно массива V_R . Все 16 пар массивов показаны в табл. 5 условно, для большей наглядности описания. Фактически достаточно задействовать только ключевую пару V_0 — V_R и сдвиги Δ .

Таблица 4

Результаты первого этапа шифрования в режиме OFB

Сдвиг Δ		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
Синхропосылка		00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
Гамма	блок 1	80	63	82	81	a0	6f	9e	5d	7c	4b	5a	49	c8	47	46	87
	блок 2	67	53	54	9a	5b	bf	3b	94	15	c4	d0	31	80	06	73	f5
	блок 3	ad	eb	2e	f5	80	3a	5f	41	26	f0	9a	e5	24	bf	f5	09
	блок 4	0a	3c	51	ed	f0	ae	29	c0	a6	37	35	6d	e8	e6	74	ce
	блок 5	02	ab	b5	2b	b2	94	e0	1b	b4	9e	b3	37	ba	c8	3c	b7
	блок 6	5b	eb	02	e3	51	70	b5	9a	9c	a9	a2	44	40	cd	6a	a5

Пошаговая зашифровка блока 1 таблицы 4

Шаг	Сдвиг Δ	Шифрующие массивы	Текст	
1	0	Ключевая пара $B_0—B_R$	до замены	00000000000000000000000000000000
			после замены	04660000000000000000000000000000
2	1	$B_1—B_R$	до замены	04660000000000000000000000000000
			после замены	04638c00000000000000000000000000
3	2	$B_2—B_R$	до замены	04638c00000000000000000000000000
			после замены	04638286000000000000000000000000
4	3	$B_3—B_R$	до замены	04638286000000000000000000000000
			после замены	04638281d00000000000000000000000
5	4	$B_4—B_R$	до замены	04638281d00000000000000000000000
			после замены	04638281a06c00000000000000000000
6	5	$B_5—B_R$	до замены	04638281a06c00000000000000000000
			после замены	04638281a06f92000000000000000000
7	6	$B_6—B_R$	до замены	04638281a06f92000000000000000000
			после замены	04638281a06f9e5b0000000000000000
8	7	$B_7—B_R$	до замены	04638281a06f9e5b0000000000000000
			после замены	04638281a06f9e5d7700000000000000
9	8	$B_8—B_R$	до замены	04638281a06f9e5d7700000000000000
			после замены	04638281a06f9e5d7c4f000000000000
10	9	$B_9—B_R$	до замены	04638281a06f9e5d7c4f000000000000
			после замены	04638281a06f9e5d7c4b5b0000000000
11	a	$B_a—B_R$	до замены	04638281a06f9e5d7c4b5b0000000000
			после замены	04638281a06f9e5d7c4b5a4800000000
12	b	$B_b—B_R$	до замены	04638281a06f9e5d7c4b5a4800000000
			после замены	04638281a06f9e5d7c4b5a49c9000000
13	c	$B_c—B_R$	до замены	04638281a06f9e5d7c4b5a49c9000000
			после замены	04638281a06f9e5d7c4b5a49c8480000
14	d	$B_d—B_R$	до замены	04638281a06f9e5d7c4b5a49c8480000
			после замены	04638281a06f9e5d7c4b5a49c8474800
15	e	$B_e—B_R$	до замены	04638281a06f9e5d7c4b5a49c8474800
			после замены	04638281a06f9e5d7c4b5a49c8474681
16	f	$B_f—B_R$	до замены	04638281a06f9e5d7c4b5a49c8474681
			после замены	80638281a06f9e5d7c4b5a49c8474687

Примечание. Заменяемые и заменяющие знаки (пары байтов) подчеркнуты

Зашифруем тот же текст с теми же начальными условиями в режиме СВС (рис. 3).

Порядок операций следующий:

- шифртекст первого блока получают контекстной заменой знаков XOR суммы синхропосылки и открытого текста блока;

- шифртексты следующих блоков получают заменой знаков XOR суммы шифртекста предыдущего блока и открытого текста текущего блока.

Результаты шифрования в этом режиме так же показаны в табл. 4, поскольку открытый текст у всех блоков 00...00.

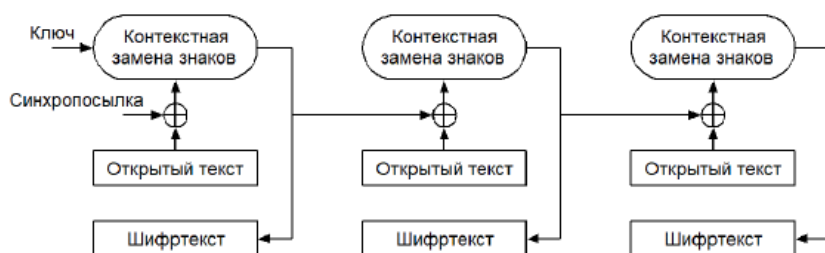


Рис. 3. Режим простой замены с сцеплением СВС

На тех же условиях зашифруем текст 00...00 в режиме CFB (рис. 4).

Зашифровка первого блока:

- выполняется контекстная замена знаков синхропосылки;
- полученный результат XORится с открытым текстом блока.

Зашифровка следующих блоков:

- выполняется замена знаков шифртекста предыдущего блока;
- полученный результат XORится с открытым текстом текущего блока.

Шифрование блоков с открытым текстом 00...00 в любом из режимов OFB, CBC и CFB даёт одни и те же результаты, показанные в табл. 4. При необходимости возможно использование любого из этих режимов для генерации гаммы.

Многопоточность

Шифр контекстной замены допускает одновременное шифрование группы блоков в нескольких потоках. Для этого достаточно в каждом потоке задать уникальную очередь сдвигов. При вводе очереди вручную они могут быть дополнительными элементами секретности. Многопоточность возможна в любом из режимов OFB, CFB, CBC, CTR, ECB. Пример одновременного шифрования пяти блоков в режиме OFB представлен в табл. 6.

Для массивов 16×16 можно задать $16! \approx 2^{44}$ очередей сдвигов. Поскольку параллельные вычисления возможны на уровне блоков, предполагается на видеокартах получить скорость шифрования соизмеримую со скоростью потоковых шифров.

В табл. 7 представлены варианты шифров контекстной замены.

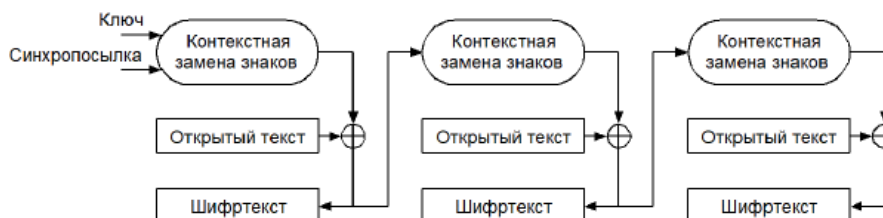


Рис. 4. Режим гаммирования с обратной связью по шифртексту CFB

Таблица 6

Одновременное шифрование пяти блоков в режиме OFB

Поток	Очередь сдвигов	Шифртекст
1	0123456789abcdef	80638281a06f9e5d7c4b5a49c8474687
2	12345678a9bcdef0	faa227150af3e8dcc9acb991887c68593
3	213456789abcdef0	2c7351808f7e1ddcabea59881746159c
4	f123456789abcde0	b34a685f8584711ad3aee2578f1c4018
5	fedcba9876534210	ae461748999acb9cadae7f8160824368

Примечание. Ключевые массивы B_0 — B_R . Блоки 128 бит. Синхропосылка 00...00. У всех блоков открытый текст 00...00. Один раунд шифрования.

Таблица 7

Варианты шифров контекстной замены

№	Размер знака алфавита или шаг замены текста, бит	Размер блока ² , бит	Число раундов ³	Размер ключевых массивов	Число пар ключевых массивов ⁴	Возможное число пар ключевых массивов
1	4	128	1	4 × 4	2 (8)	$16!^4 \approx 2^{177}$
2					4 (16)	$16!^8 \approx 2^{354}$
3	6 ¹	120	10 (5)	8 × 8	1 (8)	$64!^{12} \approx 2^{591}$
4	8	128	8 (4)	16 × 16	1 (16)	$256!^{12} \approx 2^{3367}$

Примечание. Размер ключа 128 бит. Возможны ключи большего размера кратного размеру знака алфавита, например, 256 бит. Перед шифрованием ключ расширяется до ключевых массивов [1].

¹ Пример ключевых массивов с шестибитным алфавитом (см. рис. 5). В массивах использована восьмеричная система счисления 0, 1, ..., 6, 7.

² Возможны блоки другого размера кратного размеру знака алфавита.

³ Один раунд для режимов OFB, CFB, CBC (см. раздел "Число раундов"). Для режимов ECB и CTR число раундов 16, 10, 8 при блоках 128 или 120 бит и 8, 5, 4 раунда при блоках 64 или 60 бит.

⁴ Создаются дополнительные пары за счёт постстроковой сдвижки массивов ключа. В скобках показано число пар шифрующих массивов.

C ₀								C _R							
00	01	02	03	04	05	06	07	53	27	13	07	54	62	20	73
10	11	12	13	14	15	16	17	21	55	74	71	77	36	04	60
20	21	22	23	24	25	26	27	64	43	24	46	66	30	12	52
30	31	32	33	34	35	36	37	05	75	65	25	06	50	10	47
40	41	42	43	44	45	46	47	45	63	03	00	15	22	33	67
50	51	52	53	54	55	56	57	17	35	72	42	23	34	37	14
60	61	62	63	64	65	66	67	16	56	26	51	70	01	41	40
70	71	72	73	74	75	76	77	57	02	31	61	76	44	11	32

Рис. 5. Ключевые массивы с шестибитным алфавитом

Генератор гаммы на основе шифра 1 табл. 7 представлен на рис. 6.

Начальные условия генерации:

- ключевые массивы — A₀—A_R и D₀—D_R (рис. 7);
- размер блока — 128 бит;

- синхропосылка — 0000 0000 0000 0000 0000 0000 0000 0000;
- чередование пар массивов (номера пар табл. 8) — 0123 4567 3210 7654 0246 1357 6420 7531;
- число раундов — один.

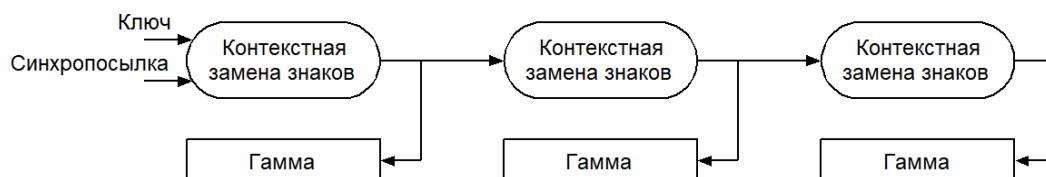


Рис. 6. Генератор гаммы

A ₀	A ₁	A ₂	A ₃	A _R
0	4	8	c	6
1	5	9	d	a
2	6	a	e	c
3	7	b	f	d
4	8	c	0	7
5	9	d	1	e
6	a	e	2	0
7	b	f	3	a
8	c	0	4	7
9	d	1	5	e
a	e	2	6	c
b	f	3	7	d
c	0	4	8	6
d	1	5	9	a
e	2	6	a	7
f	3	7	b	e

D ₀	D ₁	D ₂	D ₃	D _R
3	a	2	7	e
0	d	e	f	1
6	c	b	4	3
8	1	5	9	0
a	2	6	a	7
d	3	7	b	e
c	0	4	8	6
1	5	9	a	7
2	6	a	7	e
3	7	b	e	c
4	8	6	a	7
5	9	a	7	e
6	a	7	e	c
7	e	c	1	5
8	6	a	7	e
9	a	7	e	c

Рис. 7. Шифрующие массивы

Таблица 8

Номера пар массивов				
Пара массивов	A ₀ —A _R	A ₁ —A _R	A ₂ —A _R	A ₃ —A _R
Номер пары	0	1	2	3
Пара массивов	D ₀ —D _R	D ₁ —D _R	D ₂ —D _R	D ₃ —D _R
Номер пары	4	5	6	7

Первые 20 блоков гаммы показаны в табл. 9.

Таблица 9

Результаты генерации	
Блок	Гамма
1	28d2def62c95875d6ed9b2e0fae56e03
2	d57f66aac4d7a7974aec32eb1300f2a4
3	1b3cf610bab1d67c3dd2123fedeb18b1
4	12b54cfec3e3b6b608be1b37630a9060
5	8e2bd0b3bf09bc317032ca7221be8824
6	832fd6b57e0835d265b9504d57d49990
7	912f76f10f9c68f981e49993055ea425
8	b32070e076619d469cc309d041c16f47
9	d1e0ca9afbdea90b0a343d50ec11e22e
10	39ecf9ce6a93d43c361247b79027af12
11	18a5eb22f60302b622e787fc7ef1ea8f
12	65324f3ecf161d35dc22975abf255c6c
13	e35b7ab6727bdb5214e88462de1a36f5
14	9d30f3cc9cf3b9f8fc3e2c7d53bc5077
15	c3d56b41f31adca924365173e4a8042e
16	d70f72be93526af2d544c0a799f58f16
17	bb11b82c9210217e87a48d4c6f27edcc
18	0e340f9c828d73d669a27b55aef712d1
19	82709f499f77637f8e3d52ee4e9df61
20	98c84e6a4ca4be4f6d08dac77370b874

Для повышения скорости генерации возможно использование многопоточности (см. табл. 6). Возможно увеличение уровня секретности за счёт изменения очередности пар массивов в каждом сеансе связи. В данном случае число очередей $8!^4 \approx 2^{61}$.

Пока нет оценок длины периода такой гаммы. Рекомендуется безопасную длину задавать счётчиком (рис. 8). Если синхропосылки гамм отличаются

только одним (табл. 10) или несколькими битами, первые блоки этих гамм могут содержать одинаковые участки текстов. Для исключения таких случаев рекомендуется шифрование открытого текста начинать с 4...16 блока гаммы (в зависимости от варианта шифра, табл. 7).

Число раундов

В режимах ECB, CTR рекомендуются 4...16 раундов (табл. 7), так как при меньшем числе раундов одинаковые участки текстов разных блоков могут и в зашифрованном виде хотя бы частично остаться одинаковыми (табл. 10). В режимах OFB, CFB, CBC даже при одном раунде шифрования потока одинаковых данных такое не наблюдается (см. результаты одного раунда для потока 00...00 в табл. 4). Соседние строки в табл. 4 и 9 образуют однораундные пары "открытый текст—шифртекст". В шифрах с раундовыми ключами одной такой пары достаточно для определения ключа раунда и чтения всего шифртекста. В шифре контекстной замены это исключено, поскольку нет раундовых ключей, и каждый знак за один раунд проходит не одну, а две процедуры замены. Результат первой замены — промежуточный скрытый знак, недоступный злоумышленнику, и только вторая замена выдаёт итоговый знак.

- Замена в массиве 1: открытый знак → скрытый знак.
- Замена в массиве 2: скрытый знак → шифрзнак.

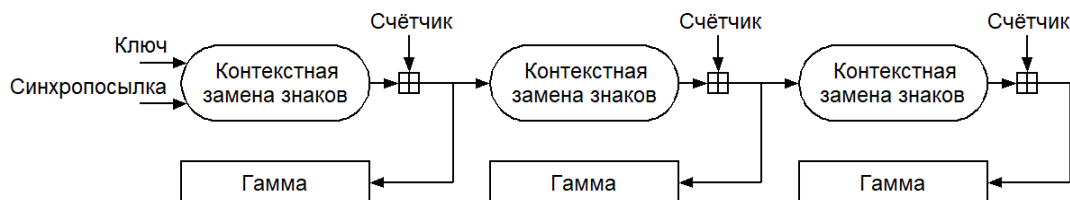


Рис. 8. Генератор гаммы со счетчиком

Таблица 10

Сравнение гамм, синхропосылки которых отличаются одним битом

Блок	Гамма 1 (табл. 9). Синхропосылка 00000000000000000000000000000000	Гамма 2. Синхропосылка 000000000000000000000000000000001
	Одинаковые участки подчеркнуты	
1	28d2def62c95875d6ed9b2e0fae56e03	d8d2def62c95875d6ed9b2e0fae56e61
2	d57f66aac4d7a7974aec32eb1300f2a4	775d66d1d4d7a7974aec32eb1300f35d
3	1b3cf610bab1d67c3dd2123fedeb18b1	dc99edbbb1d67c3dd2123fedeb9bc0
4	12b54cfec3e3b6b608be1b37630a9060	0da8ea6551e1e3282bb53867630e521d
5	8e2bd0b3bf09bc317032ca7221be8824	65f340705df4701e821b8cfbeddbadc0

- Возможно повышение уровня секретности сменой очередей сдвигов.
- Возможен прямой ввод массивов расширенного ключа.
- Отсутствуют раундовые ключи, S-блоки, сеть Фейстеля и SP-сеть.

Заключение

Шифр допускает параллельные вычисления на уровне блоков и обеспечивает высокую скорость шифрования. В режимах OFB, CFB, CBC возможно однораундное шифрование без снижения требований к криптостойкости. Поскольку шифр мало изу-

чен, нужны дополнительные доказательства его криптостойкости, особенно в случае однораундного шифрования.

Литература

1. Симон А. Б. Новое о шифре Уитстона // Вопросы защиты информации. 2020. № 2. С. 8—13.
2. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. — М.: Стандартинформ, 2015
3. Панасенко С. П. Алгоритмы шифрования: спец. справочник. — СПб.: БХВ-Петербург, 2009. С. 84—97.
4. ГОСТ 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры. — М.: Стандартинформ, 2018.

New about the Wheatstone cipher (*continuation*)

A. B. Simon

JSC "Uralmashplant", Ekaterinburg, Russia

An algorithm of symmetric block encryption based on contextual substitution of text characters is described. The cipher allows parallel calculations at the block level and provides high encryption speed. Examples of single-round encryption with a sufficient level of cryptographic strength are given.

Keywords: context, substitution, array, pair, sign, single-round, multithreaded.

Bibliography — 4 references.

Received May 10, 2023

Возможности и ограничения цифровой динамической биометрической идентификации

П. Г. Былевский, канд. филос. наук

Институт информационных наук МГЛУ (МГПИИЯ им. М. Тореца), Москва, Россия

Финансовый университет при Правительстве РФ, Москва, Россия

Проанализированы современные исследования и разработки применения биометрических данных в компьютерно-телекоммуникационных технологиях и информационной безопасности, включая оригинальные отечественные решения на основе "новой биометрии". Для улучшения выбора типа цифровых биометрических данных применительно к решаемым задачам предложена улучшенная классификация на основании видов телесных параметров: динамических и статических, контактных и дистанционных, произвольных и непроизвольных, в режиме реального времени и отложенной обработки.

Ключевые слова: биометрические данные, информационная безопасность, идентификация, классификация биометрии.

Целью статьи является определение эффективных направлений исследований и разработок использования в информационной безопасности электронных цифровых двоичных биометрических персональных данных (далее — биометрические данные), а также их относительных и уникальных преимуществ (в сравнении с техническими и организационными инструментами). Применение биометрии в информационной безопасности — всё более заметная тенденция, чаще всего для автоматизированной дистанционной идентификации пользователя. Различные биометрические решения обладают в ряде применений сравнительными и уникальными преимуществами по отношению к техническим и организационным средствам и мерам, а также друг к другу.

Широкой базой для возможного применения в информационной безопасности служат актуальные исследования и разработки в области цифрового инструментального автоматизированного выявления и идентификации состояний человеческого организма (психических и телесных, наглядно проявляющихся и внутренних, скрытых). Стартовые цели практического применения разработок часто выводят на решения, способные использо-

вать их по другим назначениям. Наблюдается динамическая взаимосвязь между предназначением разработок, выбором типов параметров человеческого организма, а также способов и оборудования оцифровки — генерации биометрических данных, их дальнейшего анализа. Улучшенная классификация различных видов биометрии способна оптимизировать выбор направлений исследований и разработок средств идентификации.

Задачи цифровой динамической биометрии

Самое большое количество исследований автоматизированного инструментального анализа и измерения психических, внутренних состояний человека наблюдают в биологии, медицине и обеспечении безопасности. В биологии человека подобными методами решают задачи инструментального количественного измерения боли [1], точного анализа качества сна [2], определения бессонницы [3]. В медицине — такими средствами пытаются выявлять предрасположенность, риски и этапы развития болезни Паркинсона [4], прогнозировать начало приступов эпилепсии [5]. В помощь тем, кому анатомически трудно или невозможно говорить, разрабатывают технические средства распознавания "внутренней" речи [6] и грамматических классов скрыто произносимых слов [7]. Непосредственно в области обеспечения безопасности идут разработки автоматизации выявления опасных состояний человека: устало-

Былевский Павел Геннадиевич, доцент кафедры "Международная информационная безопасность", доцент департамента информационной безопасности.

E-mail: pr-911@yandex.ru

Статья поступила в редакцию 3 июля 2023 г.

© Былевский П. Г., 2023

сти [8], сонливости водителей транспортных средств [9], мониторинга психологического состояния операторов ситуационных центров [10].

Задачам, связанным с безопасностью, близки исследования автоматизированного инструментального выявления, идентификации и измерения эмоций. Для решения этой задачи на основе всё тех же телесных параметров, видов биометрических данных, оборудования для их получения и способов оцифровки, применяют более сложные методы автоматизированного анализа, включая межпредметную классификацию эмоций на основе лаконичных электроэнцефалограмм (ЭЭГ) [11], использование раздельных измерений активности обоих полушарий головного мозга [12] и распознавание эмоций на перекрёстных наборах данных [13]. Также применяют вейвлет-преобразования (TQWT) для разработки автоматизированной модели классификации человеческих эмоций по ЭЭГ [14] и наиболее типичные цифровые модели эмоциональных состояний [15].

В ряде задач, для решения которых применяют цифровую биометрию, включая безопасность, оцифровка поведенческих и физиологических параметров должна быть осуществлена бесконтактными, дистанционными средствами, в том числе незаметно и без уведомления испытуемого. К таким способам и средствам сбора биометрических данных можно отнести диагностику признаков когнитивно-эмоционального конфликта во время диалога на основе видеозаписей [16] и применение для выявления скрываемого узнавания места преступления тестового моделирования посредством 3D-виртуальной реальности [17]. Новым перспективным видом специальных биометрических данных являются изменения мимики и саккадные микродвижения глаз [18], их использование открывает перспективы повышения точности результатов, в том числе для снижения противодействия выявлению обманчивого поведения.

Следует отметить, в перечисленных исследованиях контрольными биометрическими параметрами чаще всего выбраны показатели биения сердца и работы мозга на основе электрокардиограмм (ЭКГ) и ЭЭГ. Другой вид оборудования для оцифровки параметров активности мозга – контактные датчики-интерфейсы [19], в том числе для разных зон (лобных, теменных, височных и затылочных долей) [20], скальпа [21], а также имплантированный интерфейс —мозг-компьютер [22]. Полевые исследования таких параметров заведомо затруднены необходимостью постоянного контакта датчиков с телом, ограничениями режима реального времени в пользу отложенной обработки.

Новые методы генерации и анализа биометрических данных

Однако до промышленных решений доходят лишь немногие исследования в области классификации и измерения эмоций, психических, внутренних состояний человеческого организма на основании биометрических данных ЭЭГ и ЭКГ. Одна из главных причин в том, что взаимосвязь параметров функционирования мозга, сердечно-сосудистой системы с психической, сознательной деятельностью человека является скорее косвенной и неоднозначной, чем непосредственной и прямой. Параметры ЭЭГ и ЭКГ имеют не прямое, а косвенное отношение к психическим, психофизиологическим состояниям, действиям и поведению, даже к несложным движениям рук [23] или другим образам действий [24].

Дополнительные трудности обусловлены необходимостью для получения ЭЭГ и ЭКГ, во-первых, лабораторных, а не полевых условий, а во-вторых, контактных, нательных (не дистанционных) датчиков. Поэтому указанные виды биометрических данных носят частичный, слишком лаконичный характер в отношении подробности, точности выражения и определения психических, психофизиологических состояний в реальных, полевых условиях. Компенсировать эту недостаточность исследователи пытаются посредством усовершенствования математических методов и алгоритмов оцифровки (преобразования в двоичный код) и анализа (распознавания) данных.

К отдельным средствам частичного преодоления нестационарности, нелинейности и огромного разнообразия индивидуальных различий сигналов ЭЭГ можно отнести математический метод кратковременных преобразований Фурье [25]. Учитывать различные отклонения биометрических данных от контрольных параметров позволяет применение сети адаптации субъекта (SAN) на основе генеративной состязательной сети (GAN) [26]. Подобным образом многоканальную сверхточную нейронную сеть (MC-CNN) применяют для распознавания грамматического класса (глагола или существительного) скрыто произносимых слов по сигналам ЭЭГ [7]. Частично преодолеть ограничения стационарности интерфейса мозг-компьютер позволяет применение адаптивного слоя, дополнительно к слою полного соединения нейронной сети с глубокой сверткой [27]. Для распознавания эмоций по данным ЭЭГ интерфейса мозг-компьютер предлагается метод минимизации количества выборок для калибровки. Такова альтернатива предварительным длительной калибровке объекта и точной настройке "обученных"

эталонных выборок – классификационных моделей для каждого человека [19].

К новым методам распознавания эмоций человека на основе сигналов ЭЭГ путём адаптации к предметной области принадлежат состязательные дискриминационно-временные сверточные сети (AD-TCNs). Кодер временных атрибутов данных ЭЭГ создан по модели TCN, графы основных и промежуточных признаков представлены инвариантно в разных доменах [28]. Также предложен классификатор Easy Domain Adaptation (EasyDA), инвариантный к предметной области: определение на основе данных признаков эмоций по нескольким основаниям (модальностям, функциям) [29]. Характеристики многомерного сигнала ЭЭГ можно улучшено классифицировать с помощью тензорной сети с высокой способностью классификации и вычислительной эффективностью [9].

Способом уточнить распознавание эмоций по данным ЭЭГ является автоматизация выявления такого ключевого фактора, как внутренние взаимосвязи между различными каналами сигналов. Для этого разработана эффективная многоуровневая капсульная сеть с управляемыми функциями (MLF-CapsNet) для многоканального распознавания эмоций – сквозная платформа одновременного извлечения характеристик из необработанных сигналов ЭЭГ и определения эмоциональных состояний [30]. Также разработан четырехэтапный метод распознавания эмоций человека на основе многоканальных сигналов ЭЭГ. Вначале путём многомерной декомпозиции в вариационном режиме (MVMD) извлекают ансамбль многомерных модулированных колебаний (MMOs). Далее на их основе посредством функций совмещённых мгновенных амплитуды (JIA) и частоты (JIF) вычисляют многомерные частотно-временные изображения (TF). Для выявления скрытых объектов настраивается глубокая остаточная сверточная нейронная сеть ResNet-18, итоговая классификация выполняется слоем softmax [31].

Принципы классификации телесной и цифровой биометрии

Применение биометрических данных (оцифрованных телесных параметров человека) в информационной безопасности более узко, чем в других аспектах компьютерно-телекоммуникационных технологий и основано на них. Различные виды биометрических данных всё шире, разнообразнее и чаще применяют в компьютерно-телекоммуникационных решениях, в том числе в информационной безопасности, в частности, для идентификации личности и легальных пользователей.

Идентификация личности может осуществляться как в ходе непосредственного общения (осмотра, беседы и т. п., в том числе дистанционно онлайн), так и через идентифицирующие характеристики, представленные в предметах, в том числе с помощью технических средств, в документах (изображениях, описаниях и др.). Можно считать, что биометрия, в первую очередь внешний облик человека, исторически является исходным, фундаментальным средством идентификации личности. Визуальное восприятие (распознавание) может быть дополнено тактильным контактом и средствами инструментального контроля. Смена или подмена (имитация другого) внешности, привычек, имени (самозванство) с древнейших времён служила средством защиты от нежелательной верной идентификации.

Изображение личности мимикой, жестами и звуком, речевое и письменное описание индивидуальных особенностей, имя, символическое обозначение, как и предметное изображение, в рисунке или скульптуре, — производные, дистанционные во времени и пространстве обозначения за пределами места-времени непосредственного общения. Развитие производительных сил увеличивает разнообразие и расширяет применение различных технических средств (в том числе связи) для обозначения и инструментальной идентификации личности. Компьютерно-телекоммуникационные решения относят к техническим средствам представления личности, её антропометрических, биометрических и социальных характеристик и статусов (персональных данных).

В основе биометрии лежат воспринимаемые качественные и количественные индивидуальные телесные особенности (приметы), используемые для идентификации — установления, проверки, розыска личности. Индивидуальные телесные особенности, их параметры, включая доступные для инструментальных измерений и оцифровки, можно классифицировать по различным основаниям. Сами человеческие чувства подразделяют на внешние контактные — вкус, осязание и дистанционные зрение, слух и обоняние, и внутренние — проприоцепцию (мышечное чувство), боль и др.

Классификация биометрических параметров и данных производится по основанию статичность — динамика на объектные (морфологические) и процессуальные (функциональные) параметры. Существует также классификация по признаку контактности — дистанционности: параметры, доступные тактильным (и имплантированным) датчикам, кратковременным и долговременным, и которые можно измерять на расстоянии (оптическими, акустическими, электромагнитными и др. техническими

средствами). Важен фактор скорости применения биометрических данных: от режима реального времени по отношению к действиям (близко к непосредственному общению) до отложенной обработки – задержек, кратких или длительных [32]. Для снижения влияния измерительного воздействия при исследовании или в интересах безопасности можно применять классификацию по основаниям открытости или скрытности (незаметности) для измеряемого человека, в частности, возможности его уведомления и получения согласия, а также произвольности или непроизвольности (возможности сознательного контроля) действий, поведения (консервативных привычек).

К динамическим индивидуальным особенностям относят действия и поведение (почерк, походку, тембр и интонацию голоса, речевые привычки, позы, мимику и жесты), а также физиологические процессы (частота пульса, электрическая активность сердца и мозга и др.). К динамической биометрии примыкают данные пользовательской активности и о людях, генерируемые датчиками компьютерных устройств (местоположения, записи камер видеонаблюдения и т. п.). К статическим характеристикам биометрии принадлежат рост, вес, черты лица, анатомические размеры и пропорции, биохимические характеристики организма (включая ДНК). Различие двух классов особенностей безусловно: динамические могут быть стабильнее статических, которые способны сильно изменяться не только при взрослении и старении. Привычки могут изменять строение тела, а телесные формы определять физиологию и образ действий. Более корректно отмечать степень устойчивости, долговременности постоянства обоих классов.

Мобильная динамическая непроизвольная биометрия

Понимание особенностей различных видов биометрии, разнообразия их представлений в виде сведений и компьютерных данных помогает сравнивать условия их применения для различных применений. На основании этого можно принимать решения о выборе средств идентификации организационных, технических или биометрических, в последнем случае выбирать лучшие, наиболее эффективные варианты. Применение предлагаемых принципов классификации биометрии может способствовать увеличению количества эффективных доступных массовых решений, таких, как отечественный метод, названный создателями интерактивной рефлекторной биометрией [33].

Новый способ автоматизированной дистанционной идентификации пользователя создан отечественными разработчиками для современных недоверенных массово используемых мобильных устройств, смартфонов и планшетов. Идентификационным параметром является дистанционная динамическая непроизвольная (рефлекторная) биометрия – индивидуальные траектории саккадных зрительных движений зрачков. Одноразовое задание дистанционно генерируется, а данные о выполнении проверяются авторизующим центром путём сличения с индивидуальным эталоном – цифровой моделью (профилем) особенностей саккадных движений легального пользователя. Режим реального времени (интерактивный) обеспечивается анализом биометрических данных, генерируемых при получении и выполнении пользователем одноразового (по аналогу с паролями в SMS и push-уведомлениях) проверочного задания на своём мобильном устройстве.

Указанное дистанционное решение, динамическая непроизвольная биометрическая идентификация в режиме реального времени совершается на стандартной программно-аппаратной платформе массово используемых мобильных устройств [34]. Налицо заметные преимущества по сравнению с такими стандартными способами биометрической идентификации, как бесконтактной проверкой изображения, рисунка радужной оболочки глаз или контактной – отпечатков пальцев, поскольку они не верифицируют в режиме реального времени присутствие легального пользователя, сознательность выполнения им одноразового контрольного задания.

Существует потенциальная угроза имитации злоумышленниками индивидуальных особенностей саккадных движений при выполнении одноразовых проверочных заданий. Такая атака возможна посредством решения, распознающего контрольное задание и генерирующего цифровой образ саккадных движений легального пользователя, на основе управления нейросетью с актуальным дата-сетом, подобными используемым в авторизующем центре. Быстрота компьютерной имитации должна соотноситься со скоростью действий идентифицируемого человека. Однако такую угрозу следует признать гипотетической, поскольку затраты на её создание могут быть оценены как не сопоставимые с ценностью защищаемых активов владельцев массовых мобильных устройств.

Заключение

Выбор из огромного количества вариантов вида биометрических данных для оцифровки определя-

ется особенностями различных характеристик организма, а также способов и средств (оборудования и программного обеспечения) оцифровки и обработки (передачи, анализа) этих данных. Решающими факторами оказываются область применения, надёжность, удобство и стоимость биометрического решения. Классификация видов цифровой биометрии соответственно различным параметрам человеческого организма (статическим/динамическим, контактными/дистанционными, постоянными/ситуативными и т. д.) на материалах современных исследований и разработок новых решений позволяет прогнозировать продуктивные направления для цифровых технологий и информационной безопасности.

Преимущество использования биометрических данных для идентификации на недоверенных устройствах в том, что ключевые индивидуальные характеристики, используемые для их генерации, не отчуждаемы от человеческого организма, носят долговременно стабильный и произвольный характер. Уязвимость статической биометрии (цифровых образов лица, отпечатков пальца, радужной оболочки глаза и др.), широко используемой на мобильных устройствах, — отсутствие проверки наличия пользователя во время идентификации. Одним из примеров такого решения дистанционной идентификации на массовых недоверенных мобильных устройствах, является отечественная разработка — использование произвольной динамической биометрии, выполнения пользователем в режиме реального времени генерируемых одноразовых контрольных заданий.

Литература

1. Wu F., Mai W., Tang Y., Liu Q., Chen J., Guo Z. Learning Spatial-Spectral-Temporal EEG Representations with Deep Attentive-Recurrent-Convolutional Neural Networks for Pain Intensity Assessment // *Neuroscience*. 2022. V. 481. P. 144—155. DOI: 10.1016/j.neuroscience.2021.11.034.
2. Zhao R., Xia Y., Wang Q. Dual-modal and multi-scale deep neural networks for sleep staging using EEG and ECG signals // *Biomedical Signal Processing and Control*. 2021. V. 66. P. 1—10. DOI: 10.1016/j.bspc.2021.102455.
3. Qu W., Kao C., Hong H., Chi Z., Grunstein R., Gordon C., Wang Z. Single-channel EEG based insomnia detection with domain adaptation // *Computers in Biology and Medicine*. 2021. V. 139. DOI: 10.1016/j.compbiomed.2021.104989.
4. Dar M., Akram M., Yuvaraj R., Khawaja S., Murugapam M. EEG-based emotion charting for Parkinson's disease patients using Convolutional Recurrent Neural Networks and cross dataset learning // *Computers in Biology and Medicine*. 2022. V. 144. DOI: 10.1016/j.compbiomed.2022.105327.
5. Pen P., Xie L., Zhang K., Zhang J., Yang L., Wei H. Domain adaptation for epileptic EEG classification using adversarial learning and Riemannian manifold // *Biomedical Signal Processing and Control*. 2022. V. 75. DOI: 10.1016/j.bspc.2022.103555.

6. Jiménez-Guarneros M., Gómez-Gil P. Standardization-refinement domain adaptation method for cross-subject EEG-based classification in imagined speech recognition // *Pattern Recognition Letters*. 2021. V. 141. P. 54—60. DOI: 10.1016/j.bspc.2022.103555.
7. Datta S., Boulgouris N. Recognition of grammatical class of imagined words from EEG signals using convolutional neural network // *Neurocomputing*. 2021. V. 465. P. 301—309. DOI: 10.1016/j.neucom.2021.08.035.
8. Liu Y., Lan Z., Cui J., Sourina O., Müller-Wittig W. Inter-subject transfer learning for EEG-based mental fatigue recognition // *Advanced Engineering Informatics*. 2020. V. 46. DOI: 10.1016/j.aei.2020.101157.
9. Shen M., Zou B., Li X., Zheng Y., Li L., Zhang L. Multi-source signal alignment and efficient multi-dimensional feature classification in the application of EEG-based subject-independent drowsiness detection // *Biomedical Signal Processing and Control*. 2021. V. 70. DOI: 10.1016/j.bspc.2021.103023.
10. Li R., Wang L., Sourina O. Subject matching for cross-subject EEG-based recognition of driver states related to situation awareness // *Methods*. 2022. V. 202. P. 136—143. DOI: 10.1016/j.ymeth.2021.04.009.
11. Wang Y., Liu J., Ruan Q., Wang S., Wang C. Cross-subject EEG emotion classification based on few-label adversarial domain adaption // *Expert Systems with Applications*. 2021. V. 185. DOI: 10.1016/j.eswa.2021.115581.
12. Huang D., Chen S., Liu C., Zheng L., Tian Z., Jiang D. Differences first in asymmetric brain: A bi-hemisphere discrepancy convolutional neural network for EEG emotion recognition // *Neurocomputing*. 2021. V. 448. P. 140—151. DOI: 10.1016/j.neucom.2021.03.105.
13. Joshi V., Ghongade R., Joshi A., Kulkarni R. Deep BiLSTM neural network model for emotion detection using cross-dataset approach // *Biomedical Signal Processing and Control*. 2022. V. 73. <http://dx.doi.org/10.1016/j.bspc.2021.103407>.
14. Dogan A., Akay M., Barua P., Baygine M., Dogan S., Tuncer T., Dogru A., Acharya U. PrimePatNet87: Prime pattern and tunable q-factor wavelet transform techniques for automated accurate EEG emotion recognition // *Computers in Biology and Medicine*. 2021. V. 138. DOI: 10.1016/j.compbiomed.2021.104867.
15. Li Y., Fu B., Li F., Shi G., Zheng W. A novel transferability attention neural network model for EEG emotion recognition // *Neurocomputing*. 2021. V. 447. P. 92—101. DOI: 10.1016/j.neucom.2021.02.048.
16. Vartanov A., Neroznikova Y., Izbasarova S., Artamonov I., Artamonova Y., Vartanova I. Remote identification of psychophysiological parameters for a cognitive-emotional conflict // *Cognitive Systems Research*. 2022. V. 72. P. 80—87. DOI: 10.1016/j.cogsys.2021.10.006.
17. Norman D., Wade K., Watson D. Caught Virtually Lying — Crime Scenes in Virtual Reality Help to Expose Suspects' Concealed Recognition // *Journal of Applied Research in Memory and Cognition*. 2020. V. 9(1). P. 118—127. DOI: 10.1016/j.jarmac.2019.12.008.
18. Khan W., Crockett K., O'She J., Hussain A., Khan B. Deception in the eyes of deceiver: A computer vision and machine learning based automated deception detection // *Expert Systems with Applications*. 2020. DOI: 10.1016/j.eswa.2020.114341.
19. Bhosale S., Chakraborty R., Koppurapu S. Calibration free meta learning based approach for subject independent EEG emotion recognition // *Biomedical Signal Processing and Control*. 2022. V. 72. DOI: 10.1016/j.bspc.2021.103289.
20. Guo W., Xu G., Wang Y. Horizontal and vertical features fusion network based on different brain regions for emotion recognition // *Knowledge-Based Systems*. 2022. V. 247. DOI: 10.1016/j.knosys.2022.108819.

21. Jana G., Sabath A., Agrawal A. Capsule neural networks on spatio-temporal EEG frames for cross-subject emotion recognition // Biomedical Signal Processing and Control. 2022. V. 72 (Part B). DOI: 10.1016/j.bspc.2021.103361.
22. Wang Y., Qiu S., Ma X., He H. A prototype-based SPD matrix network for domain adaptation EEG emotion recognition // Pattern Recognition. 2021. V. 110. P. 1—12. DOI: 10.1016/j.patcog.2020.107626.
23. Zhang K., Robinson N., Lee S., Guan C. Adaptive transfer learning for EEG motor imagery classification with deep Convolutional Neural Network // Neural Networks. 2021. V. 136. P. 1—10. DOI: 10.1016/j.neunet.2020.12.013.
24. Zhao X., Liu D., Ma L., Liu Q., Chen K., Xie S., Ai Q. Deep CNN model based on serial-parallel structure optimization for four-class motor imagery EEG classification // Biomedical Signal Processing and Control. 2022. V. 72 (Part A). DOI: 10.1016/j.bspc.2021.103338.
25. Wang F., Wua S., Zhang W., Xu Z., Zhang Y., Wu C., Coleman S. Emotion recognition with convolutional neural network and EEG-based EFDMS // Neuropsychologia. 2020. V. 146. DOI: 10.1016/j.neuropsychologia.2020.107506.
26. Minga Y., Ding W., Pelusici D., Wu D., Wang Y., Prasad M., Lin C. Subject adaptation network for EEG data analysis // Applied Soft Computing. 2019. V. 84. DOI: 10.1016/j.asoc.2019.105689.
27. Zheng M., Yang B. A deep neural network with subdomain adaptation for motor imagery brain-computer interface // Medical Engineering & Physics. 2021. V. 96. P. 29—40. DOI: 10.1016/j.medengphy.2021.08.006.
28. He Z., Zhong Y., Pan J. An adversarial discriminative temporal convolutional network for EEG-based cross-domain emotion recognition // Computers in Biology and Medicine. 2022. V. 141. DOI: 10.1016/j.combiomed.2021.105048.
29. Chen C., Vong C., Wang S., Wang H., Pang M. Easy Domain Adaptation for cross-subject multi-view emotion recognition // Knowledge-Based Systems. 2022. V. 239. DOI: 10.1016/j.knosys.2021.107982.
30. Liu Y., Ding Y., Li C., Cheng J., Song R., Wan F., Chen X. Multi-channel EEG-based emotion recognition via a multi-level features guided capsule network // Computers in Biology and Medicine. 2020. V. 123. DOI: 10.1016/j.combiomed.2020.103927.
31. Padhmashree V., Bhattacharyya A. Human emotion recognition based on time–frequency analysis of multivariate EEG signal // Knowledge-Based Systems. 2021. V. 238. DOI: 10.1016/j.knosys.2021.107867.
32. Бродский А. В., Горбачев В. А., Карпов О. Э., Коняевский В. А., Кузнецов Н. А., Райгородский А. М., Тренин С. А. Идентификация в компьютерных системах цифровой экономики // Информационные процессы. 2018. Т. 18. № 4. С. 376—385.
33. Коняевский В. А., Тренин С. А., Абдуллаева И. А. Верификация на котлах // Защита информации. INSIDE. 2021. № 4. С. 30—37.
34. Коняевский В. А. Патент RU № 2670648 C1, СПК G06K 9/62(2006.01). Интерактивный способ биометрической аутентификации пользователя. № 2017144202. Заявл. 2017.12.18. Оpubл. 2018.10.24. Бюл. № 30, 24.10.2018.

Possibilities and limitations of digital dynamic biometric identification

P. G. Bylevsky

Institute of Information Sciences of MGLU (MGPIIYa named after M. Torez), Moscow, Russia
Financial University under the Government of the Russian Federation, Moscow, Russia

The article analyzes modern research and development of the use of biometric data in computer and telecommunications technologies and information security, including original domestic solutions based on "new biometrics". To improve the choice of the type of digital biometric data in relation to the tasks being solved, an improved classification is proposed based on the types of bodily parameters: dynamic and static, contact and remote, arbitrary and involuntary, real-time and deferred processing.

Keywords: biometric data, information security, identification, classification of biometrics.

Bibliography — 34 references.

Received July 3, 2023

Разработка метода генерации речеподобной помехи с применением фонов идентифицированного по голосу диктора

^{1, 2} Р. А. Васильев, канд. техн. наук; ² Д. А. Ляхманов, канд. техн. наук;

² С. Н. Капранов, канд. техн. наук

¹ Акционерное общество "Финансы, Информация, Технология" (АО "ФИНТЕХ"), Москва, Россия

² Нижегородский государственный технический университет им. Р. Е. Алексеева, г. Нижний Новгород, Россия

Рассмотрены особенности использования речеподобной помехи (РЧП) для защиты конфиденциальных переговоров. Предложен метод генерации РЧП с возможностью идентификации голоса диктора и применения его фоном для генерации РЧП. Описана программная реализация предложенного метода — "Информационная система идентификации дикторов по голосу" (ИС ИДГ), модернизированная под задачи генерации РЧП с применением фоном идентифицированного по голосу диктора.

Ключевые слова: речеподобная помеха, идентификация диктора по голосу, словесная разборчивость речи, цифровая шумоочистка.

Защита акустической информации, циркулирующей в защищаемом помещении, входит в один из базисов мероприятий по информационной безопасности предприятия (организации, фирмы). Данные мероприятия реализуют с применением пассивных и активных методов защиты [1].

Пассивные методы защиты строятся на основе снижения вероятности получения информации или ее расшифровки из акустических источников с использованием различного вида звукопоглощающих материалов, используемых во время проведения строительных работ, связанных с возведением или реконструкцией капитального строения.

Активные методы защиты акустической информации — это методы, при которых используют специальное оборудование или программно-аппаратные комплексы, для предотвращения утечки акустической информации. Активные методы основаны на создании дополнительных помех, которые скрывают сигнал, несущий речевую

информацию, в каналах, где может быть утечка. В качестве маскирующих сигналов широко используют "белый" или "розовый" шум с диапазоном частот от 100 до 10000 Гц [2].

В последнее время начали применяться и комбинированные сигналы, включающие один из упомянутых и так называемые речеподобные сигналы. Наилучшие результаты можно получить при использовании сигналов, близких по спектральному составу к охраняемым и имеющим структуру речевого сообщения [3—6].

Авторами предложен алгоритм формирования речеподобной помехи, представляющей собой случайную последовательность звуков речи с возможностью идентификации голоса диктора с применением метода обесцвечивающего фильтра [7]. Алгоритм формирования речеподобной помехи реализован с использованием программного средства разработки MatLab в разработанной автором "Программе идентификации дикторов по голосу" (ИС ИДГ) [8], модернизированной для решения задачи генерации речеподобной помехи диктора. Эффективность предлагаемой речеподобной помехи оценена экспериментально.

Теоретический анализ

Для защиты конфиденциальных переговоров часто применяют устройства активной защиты речевой информации, как правило, состоящей из генератора маскирующих сигналов и набора преобразователей электрических сигналов в акусти-

Васильев Роман Александрович, доцент, начальник отдела аудита информационной безопасности Департамента информационной безопасности.

E-mail: r.vasilev@fintech.ru

Ляхманов Дмитрий Александрович, доцент кафедры "Информационная безопасность вычислительных систем и сетей".

E-mail: dm.virger@gmail.com

Капранов Сергей Николаевич, доцент кафедры "Информатика и системы управления".

E-mail: serg.kapranov@gmail.com

Статья поступила в редакцию 2 июня 2023 г.

© Васильев Р. А., Ляхманов Д. А., Капранов С. Н., 2023

ческие (например, электродинамических громкоговорителей) или преобразователей электрических сигналов в механические перемещения. В табл. 1 приведены характеристики наиболее распространенных средств защиты речевой информации от утечки по акустическим каналам.

Проведенные исследования показали, что наиболее эффективным является речеподобная помеха, формируемая из речевых сигналов [9].

Речеподобный сигнал — это звуковой сигнал, который имитирует речь и предназначается для передачи сообщения или информации между людьми или машинами. Речеподобные сигналы характеризуются сильной корреляцией с человеческой речью, содержат явные фонетические и интонационные признаки и имеют определенный формат данных. Речеподобная помеха — это синтезируемый по случайному закону акустический сигнал, который по своим основным характеристикам соответствует речевому сигналу, но не содержит смысловой информации.

На данный момент времени специалистами предлагается три типа формирования речеподобной помехи (РЧП):

- в РЧП 1-го типа производится формирование из N -го количества речи дикторов открытого

радиовещания при равномерном сложении этих звуковых дорожек;

- в РЧП 2-го типа производится формирование из 1-го осинового речевого сигнала или используется микширование музыкальных фрагментов и речевых сигналов дикторов радиовещания с определенным шумом;

- в РЧП 3-го производится формирование из скрываемого речевого сигнала при большом количестве наложений данного же речевого сигнала различного уровня.

В монографии "Расчет и измерение разборчивости речи" (1962 г.) Н. Б. Покровского была описана теория разборчивости речи, а также представлен сравнительный анализ различных способов оценки качества передачи сигнала. Основным показателем эффективности защиты речевого сигнала является словесная разборчивость речи W_c .

Словесная разборчивость W_c показывает насколько понятна для оператора технических систем перехвата информации очищенный речевой сигнал от систем защиты акустической информации. Для расчёта словесной разборчивости W_c выполняют следующие описанные ниже операции.

Таблица 1

Характеристики средств активной защиты речевой информации

Наименование	Диапазон рабочих частот, Гц	Вид маскирующих сигналов	Число каналов	Производитель
"Прибой"	100—8000	"Белый" шум	4	Беларусь
"Прибой-Р"	100—8000	"Белый" шум + речеподобные сигналы	4	Беларусь
ANG-2000	250—5000	"Белый" шум	1	США
WNG-023	100—12000	"Белый" шум	1	Россия
"Шорох-2М"	100—12000	"Белый" шум	1	Россия
"Порог-2М"	250—5000	"Белый" шум	1	Россия
VNG-006/ VNG-012GL	400—5000	"Белый" шум	5	Россия
"Барон"	90—11200	"Белый" шум + речеподобные сигналы	4	Россия
СТБ231 "Бирюза"	90—11200	"Белый" шум	3	Россия
ЛГШ-402	Нет данных	"Белый" шум	2	Россия

Спектр речи разбивают на N -е количество октавных полос, в частных случаях произвольных, чаще всего используют среднегеометрические частоты в диапазоне от 250 Гц до 4000 Гц.

Для каждой частотной полосы определяется показатель ΔA_i , показывающий энергетическую избыточность дискретной составляющей речевого сигнала. Под избыточностью принято принимать наличие в речи неформатных составляющих (основной тон и т. д., зависящие от индивидуальных показателей диктора), так же рассчитывается весовой коэффициент k_i (k_i — показывает наличие форманты речи в частотной полосе).

Производится расчёт q_i для N -й октавной полосы, q_i есть не что иное как уровень речевого сигнала к уровню шума. Используя q_i , возможно посчитать коэффициент восприятия слухового аппарата человека p_i — это предположительное количество формантных речи, которые имеют показатель выше предельного значения восприятия. Далее рассчитывается спектральный индекс разборчивости речи R_i и интегральный индекс артикуляции речи R . После расчёта основных показателей для определения словесной разборчивости речи W_c полученный индекс артикуляции речи подставляется в формулу расчёта W_c [10].

$$W_c = \begin{cases} 1,54 \cdot R^{0,25} [1 - \exp(-11 \cdot R)], & \text{если } R < 0,15; \\ 1 - \exp\left(-\frac{11 \cdot R}{1 + 0,7 \cdot R}\right), & \text{если } R \leq 0,15. \end{cases}$$

Исследования показывают, что при W_c менее:

- 50—70 % — невозможно полностью восстановить информационную составляющую разговора;
- 20—40 % — невозможно установить тему разговора;
- 20 % — факт ведения разговор становится под вопросом.

Главная идея предложенного в статье алгоритма формирования РЧП с возможностью идентификации голоса диктора заключается не только в

снижении коэффициента словесной разборчивости W_c , используемого для расчёта выполнения норм по противодействию речевой разведки при проведении конфиденциальных переговоров, но и значительное затруднение проведения цифровой шумочистки (использование специального программного обеспечения может существенно понизить уровень шума и увеличить разборчивость речи на фоне шумов) перехваченного речевого сигнала, так как для генерации помехового сигнала используется не "белый шум", а РЧП с фонемами говорящего на совещании диктора.

Программа экспериментальных исследований

Для экспериментальных исследований была использована ранее разработанная и проверенная ИС ИДГ [11—13], модернизированная к задачам генерации РЧП диктора, посредством доработки модуля идентификации диктора по голосу, реализованный в ИС ИДГ алгоритм генерации речеподобных помех с идентификацией диктора по голосу изображен на рис. 1. Интерфейс ИС ИДГ с функцией автоматического режима работы с записью голоса, идентификацией и генерацией РЧП с использованием фонем идентифицированного диктора, представлен на рис. 2.

Экспериментальные исследования, состоящие из четырех этапов, представлены в табл. 2.

Для проведения экспериментальных исследований применяют персональную электронно-вычислительную машину (ПЭВМ), функционирующую на базе операционной системы Windows 7/10, подключенный к ПЭВМ микрофон и аудио излучатель.

В первом эксперименте при создании фонетической базы были записаны голоса 10 дикторов, в ИС ИДГ был произведен анализ и сегментация фонем, каждая фонема была названа в соответствии с первой буквой в имени диктора, например, одна из реализаций фонемы "Ы" пользователя "Васильев Роман" названа "ЫЗ-Р", и соответственно фонема "А" диктора "Николаева Надежда" — "А1-Н". На рис. 3 изображен принцип занесения фонем в голосовую базу ИС ИДГ.

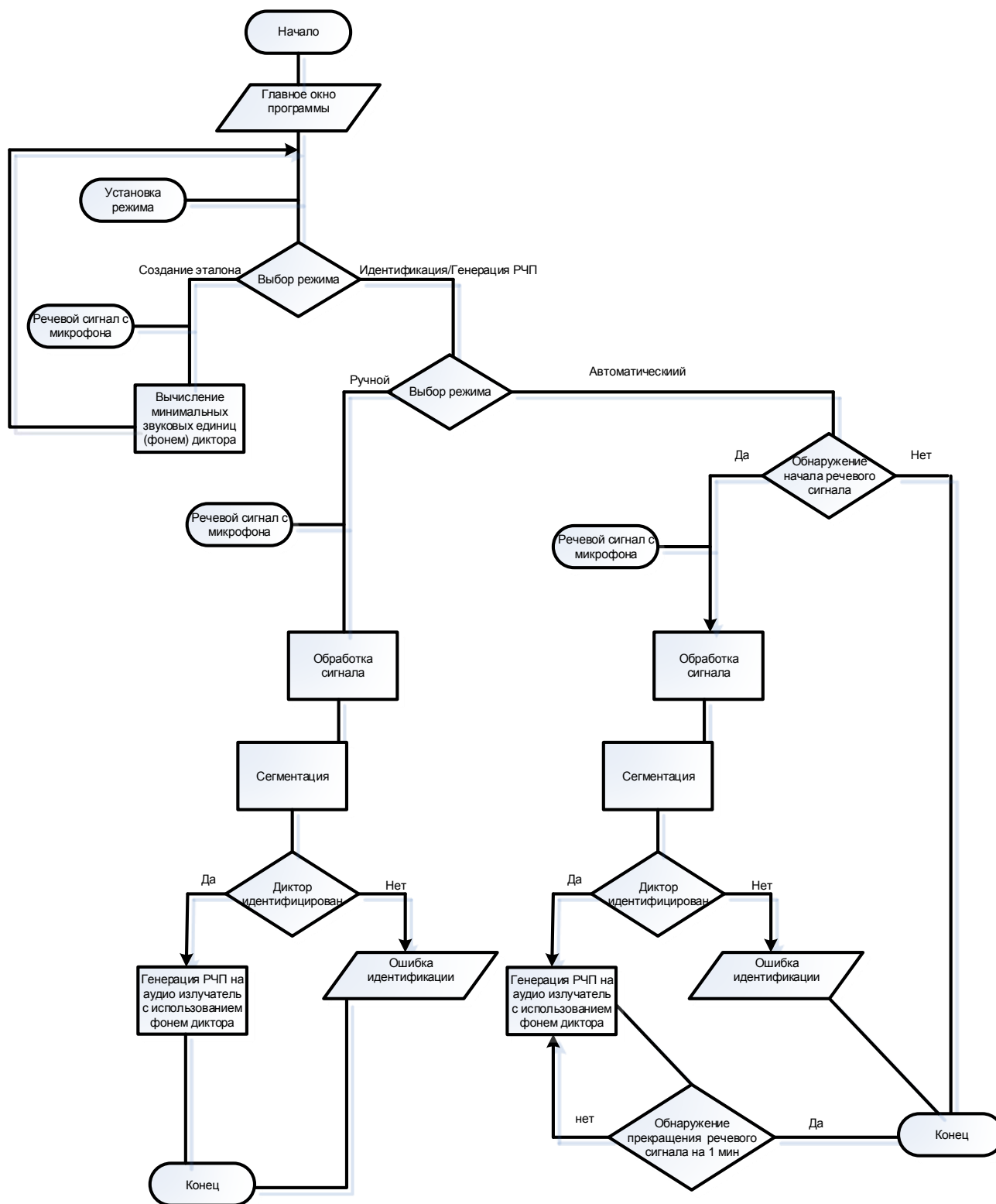


Рис. 1. Алгоритм генерации речеподобных помех с идентификацией диктора по голосу

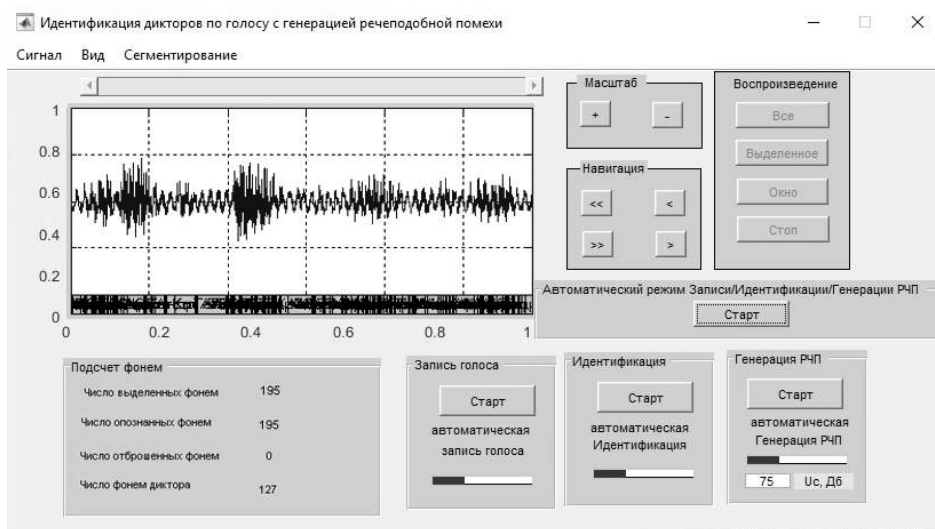


Рис. 2. Интерфейс ИС ИДГ с функцией автоматического режима работы с записью голоса, идентификацией и генерацией РЧП

Таблица 2

Этапы экспериментальных исследований

Номер эксперимента	Цель	Результаты
1	Создание базы фонем диктора и проведение процедуры идентификации по голосу	Записаны голоса 10 дикторов, произведен анализ и сегментация фонем, произведена успешная идентификация конкретного диктора во время проведения конфиденциальных переговоров из общей базы фонем
2	Генерация РЧП диктора	Выполнена успешная генерация РЧП, с использованием фонем ранее идентифицированного диктора, на аудио излучатель с заданным уровнем сигнала
3	Измерение акустического сигнала и расчет коэффициента словесной разборчивости W_c в различных условиях	Выполнено измерение акустического сигнала и расчёт коэффициента словесной разборчивости W_c : <ul style="list-style-type: none"> • без применения средств виброакустической защиты (СВАЗ) — норма W_c не выполнялась; • с применением СВАЗ, генерирующей помеху "белый шум" — норма W_c выполнялась; • с применением разработанного алгоритма генерации РЧП, реализованного в модернизированном программном обеспечении ИС ИДГ — норма W_c выполнялась
4	Очистка речевого сигнала от помехи	Выполнена цифровая шумочистка записанного речевого сигнала, модулированного "белым шумом" и РЧП диктора — при применении "белого шума" успешно выполнена очистка сигнала и содержание разговора перехвачено; с применением РЧП диктора — очистка не дала результата, содержание конфиденциального разговора не перехвачено

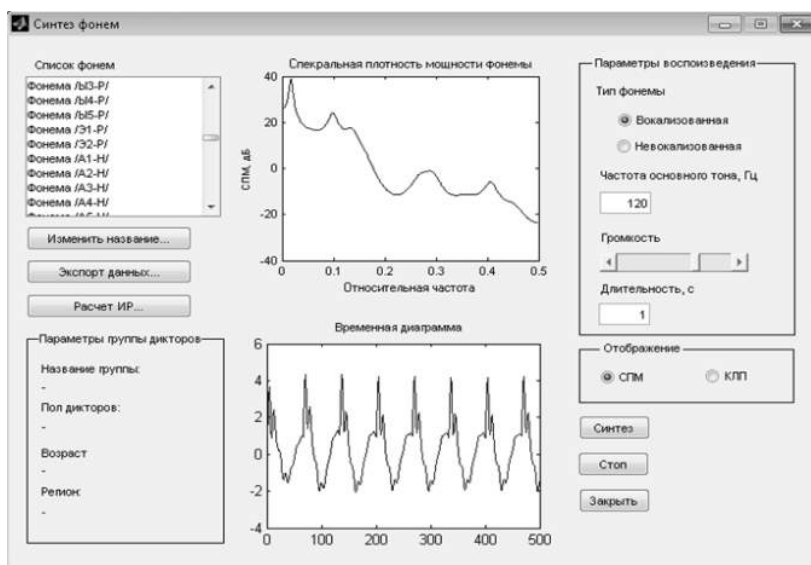


Рис. 3. Принцип занесения фонем в голосовую базу ИС ИДГ

Далее, после создания фонетической базы дикторов, в режиме реального времени выполнена запись голоса диктора и его последующая сегментация для определения принадлежности фонем и идентификации. На рис. 4 показано, что в произнесенной фразе определено 127 фонем, принадлежащих конкретному диктору, что составляет более 60 % от общего количества фонем (195) данного диктора, записанного в базу данных, что позволяет нам идентифицировать диктора "Васильев Роман".

Во втором эксперименте выполнена генерация РЧП с подачей на аудиопередатчик в хаотичном порядке всех 195 выделенных фонем, записанных в голосовую базу, ранее идентифицированного диктора, при заданном уровне акустического сигнала в 75 Дб (рис. 5). При необходимости генерации РЧП другого диктора выполнена новая запись голоса с последующей процедурой идентификации диктора и генерации РЧП с фонемами нового диктора.

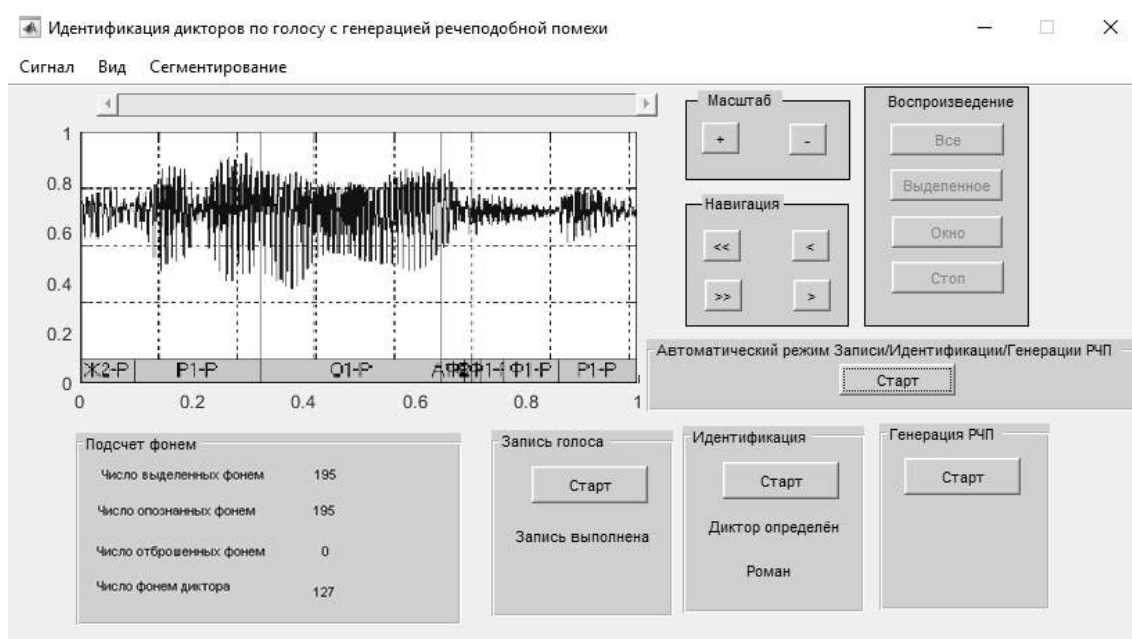


Рис. 4. Успешная идентификация диктора "Васильев Роман"

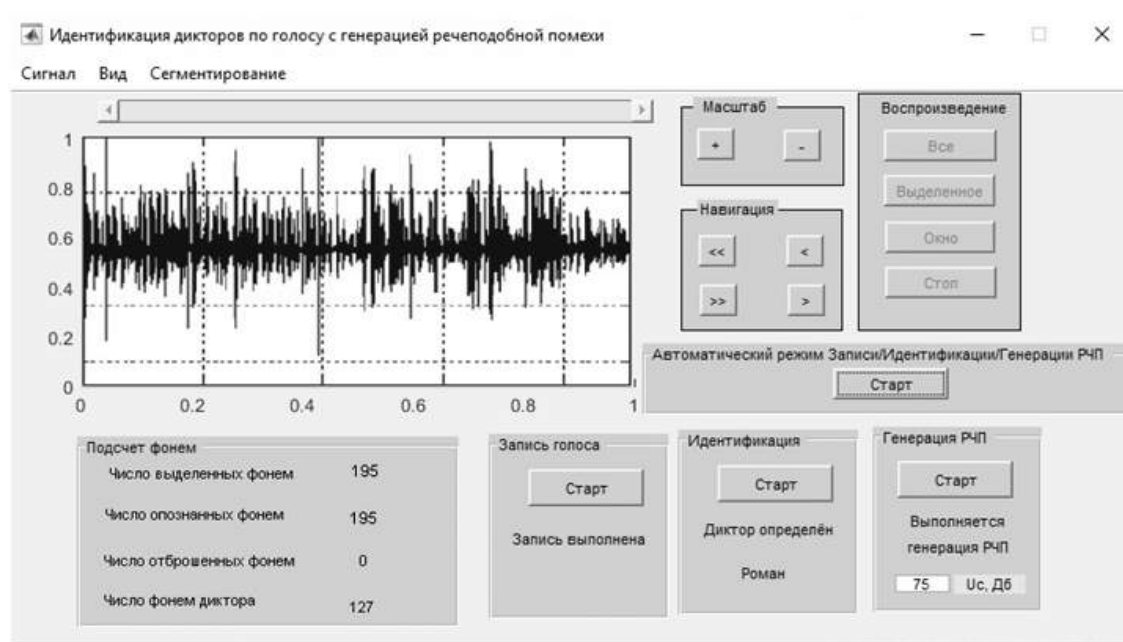


Рис. 5. Генерация РЧП фонем ранее идентифицированного диктора

Так же предусмотрен автоматический режим работы ИС ИДГ (рис. 2), при котором ИС ИДГ должна иметь взаимодействие с микрофоном, в который говорит диктор, и при начале доклада произносится тестовая фраза, к примеру "Приветствую коллеги, готов начать свой доклад". После чего делается пауза в несколько секунд, чтобы ИС ИДГ провела в автоматическом режиме обработку записанной тестовой фразы диктора, затем идентификацию диктора по голосу, далее начинается генерация РЧП на аудиоизлучатель с фонемами диктора, после чего диктор может начать конфиденциальный разговор. После окончания доклада, диктор делает минутную паузу, при этом ИС ИДГ обнаруживает, что в микрофон не подаются речевые сигналы, перестает генерировать РЧП и переходит в режим обнаружения голоса нового диктора для последующего повторения алгоритма (рис. 1).

В третьем эксперименте с применением системы оценки защищенности помещений по виброакустическому каналу "ШЕПОТ" (рис. 6), выполнено измерение акустического речевого

сигнала, поданного на звуковую колонку с ПЭВМ, и расчёт коэффициента словесной разборчивости W_c [14]. При измерениях оценивали вероятность перехвата речевой информации за счёт непреднамеренного прослушивания за дверным проёмом, расчёт W_c производил в трех режимах:

- без применения средств активной защиты речевой информации (САЗ);
- с применением акустического излучателя САЗ "Шорох-2М", генерирующего помеху "белый шум";
- с применением разработанного алгоритма генерации РЧП, реализованного в модернизированном программном обеспечении ИС ИДГ, установленного на ПЭВМ с подключенным микрофоном и акустическим излучателем.

Проведено измерение акустического сигнала в контрольной точке "дверной проём" без применения САЗ (табл. 3).

Отношение сигнал/шум не выполняется во всех октавных полосах. Произведен расчет словесной разборчивости речи W_c , норма не выполнена (табл. 4).

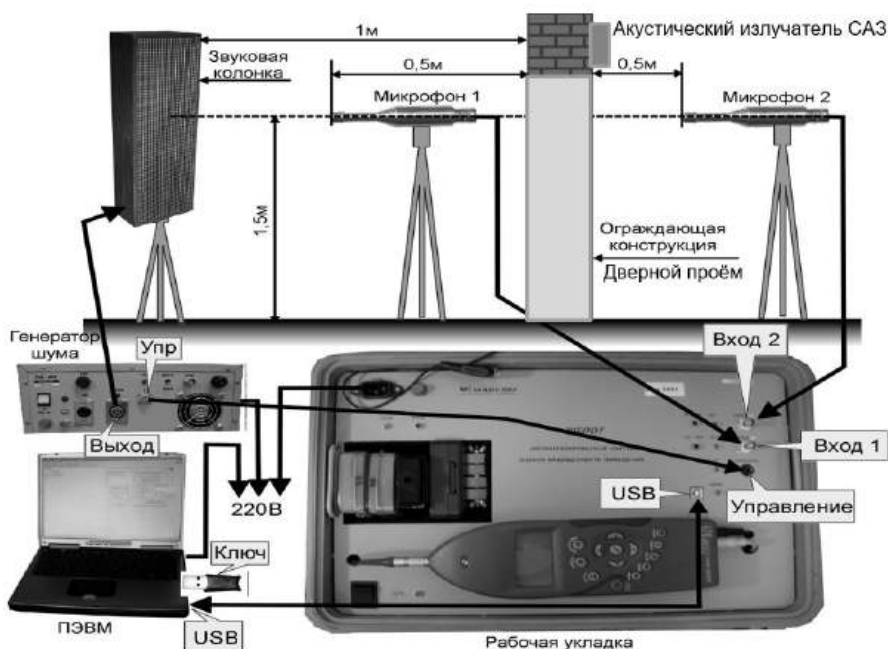


Рис. 6. Стенд для оценки защищённости речевой информации от утечки по акустическому каналу

Таблица 3

Измерение акустического сигнала без применения САЗ

№ октавной полосы	Уровень звукового давления тестового сигнала L_t , дБ	Уровень акустического шума $L_{ш}$, дБ	Уровень акустического сигнала и акустического шума $L_c + ш$, дБ	Уровень акустического сигнала L_c , дБ	Отношение сигнал/шум E_i , дБ	Соответствие нормированным отношениям сигнал/шум
1	88,30	40,70	75,90	75,90	12,90	Не выполнено
2	89,40	40,30	75,10	75,10	11,40	Не выполнено
3	88,60	42,90	76,00	76,00	5,50	Не выполнено
4	87,40	35,70	70,80	70,80	3,70	Не выполнено
5	86,50	39,40	74,90	74,90	2,00	Не выполнено

Таблица 4

Расчет словесной разборчивости речи W_c без применения САЗ

№ октавной полосы	Значение октавного индекса артикуляции r_i	Значение интегрального индекса артикуляции R	Значение показателя противодействия W_c	Выполнение нормы противодействия
1	0,0102	0,3711	0,961	Не выполнено
2	0,0501			
3	0,0777			
4	0,1280			
5	0,1051			

Проведено измерение акустического сигнала в контрольной точке "дверной проём" с применением САЗ (табл. 5).

Отношение сигнал/шум не выполнено в двух октавных полосах. Произведен расчет словесной разборчивости речи W_c , норма выполнена (табл. 6).

Проведено измерение акустического сигнала в контрольной точке "дверной проём" с применением разработанного алгоритма генерации РЧП (табл. 7).

Отношение сигнал/шум выполнено во всех октавных полосах. Произведен расчет словесной разборчивости речи W_c , норма выполнена (табл. 8).

Таблица 5

Измерение акустического сигнала с применением САЗ

№ октавной полосы	Уровень звукового давления тестового сигнала L_T , дБ	Уровень акустического шума и САЗ $L_{ш}$, дБ	Уровень акустического сигнала и акустического шума $L_c + ш$, дБ	Уровень акустического сигнала L_c , дБ	Отношение сигнал/шум E_i , дБ	Соответствие нормированным отношениям сигнал/шум
1	89,40	55,90	76,20	76,20	-3,10	Выполнено
2	90,50	55,00	75,40	75,40	-4,10	Не выполнено
3	89,70	54,90	76,30	76,30	-7,30	Не выполнено
4	88,50	55,80	71,10	71,10	-17,20	Выполнено.
5	87,60	57,40	75,20	75,20	-16,80	Выполнено

Таблица 6

Расчет словесной разборчивости речи W_c с применением САЗ

№ октавной полосы	Значение октавного индекса артикуляции r_i	Значение интегрального индекса артикуляции R	Значение показателя противодействия W_c	Выполнение нормы противодействия
1	0,0012	0,0459	0,283	Выполнено
2	0,0084			
3	0,0184			
4	0,0084			
5	0,0095			

Таблица 7

Измерение акустического сигнала с применением РЧП

№ октавной полосы	Уровень звукового давления тестового сигнала L_T , дБ	Уровень акустического шума и РЧП $L_{ш}$, дБ	Уровень акустического сигнала и акустического шума $L_c + ш$, дБ	Уровень акустического сигнала L_c , дБ	Отношение "сигнал/шум" E_i , дБ	Соответствие нормированным отношениям сигнал/шум
1	88,30	63,10	75,90	75,90	-9,50	Выполнено
2	89,40	62,20	75,10	75,10	-10,50	Выполнено
3	88,60	62,10	76,00	76,00	-13,70	Выполнено
4	87,40	63,00	70,80	69,80	-24,60	Выполнено
5	86,50	64,60	74,90	74,90	-23,20	Выполнено

Расчет словесной разборчивости речи W_c с применением РЧП

№ октавной полосы	Значение октавного индекса артикуляции, r_i	Значение интегрального индекса артикуляции, R	Значение показателя противодействия, W_c	Выполнение нормы противодействия
1	0,0003	0,0131	0,070	Выполнено
2	0,0026			
3	0,0062			
4	0,0016			
5	0,0024			

По результатам третьего эксперимента можно сделать вывод, что эффективность разработанного алгоритма генерации РЧП не только не уступает методам генерации помехи "белый шум", но и выдаёт более высокие результаты при расчёте показателя противодействия словесной разборчивости речи W_c .

В четвертом эксперименте, с применением программного обеспечения *Audacity*, выполнена цифровая шумочистка записанного речевого сигнала, модулированного "белым шумом" (рис. 7), где верхняя строка — модулированный "белым шумом" речевой сигнал, а нижняя строка — очи-

щенный речевой сигнал и шумочистка речевого сигнала, модулированного РЧП диктора (рис. 8), где верхняя строка модулированный РЧП речевой сигнал, нижняя строка — очищенный речевой сигнал.

По результатам четвертого эксперимента можно сделать вывод, что при применении "белого шума" возможно выполнение очистки сигнала и перехват содержания разговора. Цифровая шумочистка речевого сигнала, модулированного РЧП диктора, не дала результата, содержание конфиденциального разговора не перехвачено.

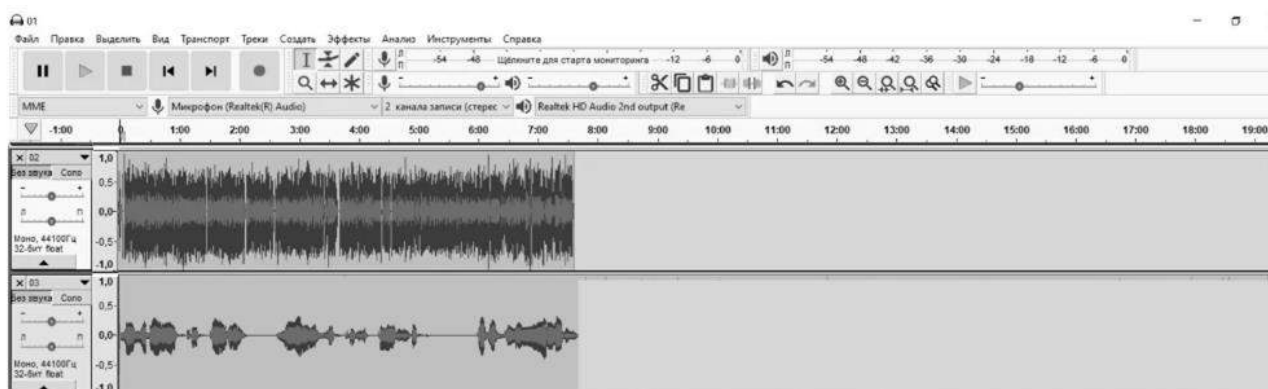


Рис. 7. Цифровая шумочистка речевого сигнала, модулированного "белым шумом"



Рис. 8. Цифровая шумочистка речевого сигнала, модулированного РЧП диктора

Закключение

Предложен метод формирования речеподобной помехи, представляющей собой случайную последовательность звуков речи идентифицированного ранее диктора. Эффективность предлагаемой речеподобной помехи оценена экспериментально, показаны преимущества разработанного алгоритма генерации РЧП с идентификацией голоса диктора по сравнению с другими методами формирования помех акустического сигнала [15].

Литература

1. Хорев А. А. Способы защиты выделенных помещений от утечки речевой (акустической) информации по техническим каналам: системы виброакустической защиты // Специальная техника. 2013. № 4. С. 31—63.
2. Хорев А. А. Системы виброакустической маскировки // Специальная техника. 2003. № 6. С. 28—33.
3. Дворянkin С. В., Уленгов С. В., Устинов Р. А., Дворянkin Н. С., Антипенко А. О. Системное моделирование речеподобных сигналов и его применение в сфере безопасности, связи и управления // Безопасность информационных технологий. 2019. Т. 26. № 4. С. 101—119.
4. Авдеев В. Б., Трушин В. А., Кунгуров М. А. Унифицированная речеподобная помеха для средств активной защиты речевой информации // Тр. СПИИРАН. 2020. Вып. 19. Т. 5. С. 991—1017.
5. Хорев А. А., Царев Н. В. Способ и алгоритм формирования речеподобной помехи // Вестник ВГУ. Сер. Системный анализ и информационные технологии. 2017. № 1. С. 57—67.
6. Воробьев В. И., Давыдов А. Г. Синтез речеподобных сигналов // Акустический журнал. 2002. № 5. Т. 48. С. 701—704.
7. Савченко В. В. Информационная теория восприятия речи // Изв. вузов России. Радиоэлектроника. 2007. Вып. 6. С. 3—9.
8. Васильев Р. А. Свид. о гос. регистрации программы для ЭВМ № 2015663306. Программа идентификации дикторов по голосу. Зарег. 15.12.2015. — М.: Роспатент, 2015.
9. Хорев А. А. Безопасность информационных технологий [Электронный ресурс]. 2008. Режим доступа: http://www.security.ukrnet.net/d-book-2/ch_10.pdf. (дата обращения: 28.04.2023).
10. Покровский Н. Б. Расчет и измерение разборчивости речи. — М.: Гос. изд-во лит. по вопросам связи и радио, 1962. — 391 с.
11. Васильев Р. А., Ротков Л. Ю. Адаптация метода биометрической идентификации по голосу к тихому произнесению парольных фраз для противодействия утечки речевой информации по акустическим каналам: тр. XXV научной конференции по радиофизике. — Нижний Новгород: ННГУ, 2021. С. 517—524.
12. Васильев Р. А. Исследование фонетического строя речи и идентификация дикторов по голосу // Вопросы защиты информации. 2013. № 1(100). С. 43—51.
13. Васильев Р. А. Адаптация метода биометрической идентификации по голосу к тихому произнесению парольных фраз для противодействия акустической речевой разведке // Вопросы защиты информации. 2021. № 1(132). С. 33—39.
14. Васильев Р. А., Ротков Л. Ю. Оценка защищенности речевой информации от утечки по акустическим и виброакустическим каналам с помощью программно-аппаратного комплекса "Шёпот": учеб.-метод. пособие, ННГУ, 2020. — 57 с.
15. Асеев Г. Д., Антасов И. С. Оценка эффективности применения шумовых "речеподобных" помех для защиты акустической информации // Вестник УрФО. 2018. № 2(28). С. 19—24.

Development of a method for generating speech-like noise using phonemes identified by the speaker's voice

^{1,2} R. A. Vasiliev, ² D. A. Lyakhmanov, ² S. N. Kapranov

¹ Joint Stock Company "Finance, Information, Technology" (JSC "FINTECH"), Moscow, Russia

² Nizhny Novgorod State Technical University n. a. R. E. Alekseev, Nizhny Novgorod, Russia

The features of the use of speech-like interference (RFI) for the protection of confidential negotiations are considered. A method for generating RFI with the possibility of identifying the speaker's voice and using his phonemes to generate RFI is proposed. The software implementation of the proposed method is described — "Information System for Identification of Speakers by Voice" (IS IDG), modernized for the tasks of generating RFI using phonemes of the speaker identified by voice.

Keywords: speech-like interference, speaker identification by voice, verbal speech intelligibility, digital noise cleaning.

Bibliography — 15 references.

Received June 2, 2023

Аналитическое исследование проблемы биометрической идентификации и аутентификации субъектов по голосу

Д. П. Иниватов

ФГАОУ ВО «Омский государственный технический университет», Россия, Омск

Представлен обзор современных достижений и методов в области распознавания человека по голосу и биометрической идентификации. Рассматриваются ключевые задачи, с которыми сталкиваются исследователи в этой области, такие, как борьба с шумом, дрейфом голосовых характеристик, спуфингом и состязательными атаками, диаризация и др. Приводятся сравнительные таблицы результатов исследований, проведенных в этой области. Особое внимание уделяется прогрессу в разработке методов, способных улучшить точность распознавания голоса в условиях шума и переменных голосовых характеристик. В обзоре приводятся наиболее значимые результаты из достигнутых на сегодняшний день и очерчен круг актуальных (нерешенных) проблем. Отмечается, что перспективным направлением можно рассматривать реализацию различных архитектур, включающих в себя нейросетевой преобразователь биометрия-код с целью защиты биометрических шаблонов.

Ключевые слова: автоматическое распознавание говорящего, глубокое обучение, спуфинг, противодействие шуму, параметры голоса диктора, биометрическая аутентификация, корпуса голосовых данных.

В современном информационном обществе обеспечение безопасности данных становится важнейшей задачей. Одним из эффективных и перспективных способов подтверждения личности является использование биометрических технологий. Среди различных биометрических параметров голос является одним из самых удобных и широко распространенных способов идентификации.

Глобальный рынок голосовой биометрии активно расширяется. Прогнозы и исследования в данной отрасли подтверждают постоянный рост спроса на такие технологии [1]. Ведущие компании, специализирующиеся на голосовой биометрии, активно инвестируют в исследования и разработку новых методов для повышения эффективности и надежности систем.

Однако, несмотря на прогресс в этой области, остаются актуальными проблемы, связанные с использованием голоса для подтверждения личности и проверки подлинности пользователей. С ростом популярности биометрии возникают вопросы надежности, безопасности и устойчивости. Злоумышленники могут попытаться подделать голосовую информацию или провести атаки на системы с целью несанкционированного доступа.

Статистические данные подтверждают значимость проблемы, что указывает на рост числа кибератак и нарушений безопасности в различных секторах. Исследования, проведенные компанией IBM Security и Ponemon Institute, демонстрируют, что средняя стоимость нарушения безопасности на уровне компаний, включая затраты на реагирование на инцидент, восстановление и потерю деловой активности, достигает 4,35 миллионов долларов [2].

Данная работа имеет цель рассмотреть существующие методы к голосовой аутентификации, оценить подходы к повышению точности, существующие наборы речевых данных, а также проанализировать проблемы в этой области.

Защита биометрических данных от компрометации на этапах хранения и исполнения

Для осуществления надежной сохранности биометрических шаблонов применяют множество методов: различные виды шифрования, многофакторная аутентификация, системы контроля доступа и многие другие [3]. Важно учитывать потенциальные риски утечки биометрических параметров и принимать меры для их устранения или снижения. Раскрытие подобной информации способно привести к серьезным угрозам с безопасностью. Как подчеркнула сооснователь компании «Лабо-

Иниватов Даниил Павлович, ассистент.
E-mail: daniilini@mail.ru

Статья поступила в редакцию 5 сентября 2023 г.

© Иниватов Д. П., 2023

ратория Касперского» Наталья Касперская [4], биометрические данные невозможно изменить, в отличие от паролей и других методов аутентификации. При осуществлении данной процедуры необходимо обеспечить защиту знаний, к которым относятся пароли, секретные ключи, а также биометрические параметры, применяемые для задачи подтверждения личности субъекта.

Важно обеспечить сохранность указанной информации на всех этапах её использования: начиная от этапа сбора и регистрации пользовательских данных, до этапа их хранения и обработки в рамках процедуры аутентификации [5]. Одним из методов защиты знаний является хранение их в зашифрованном виде. Существует несколько подходов к шифрованию включая классическое и гомоморфное.

Несмотря на то, что классическое шифрование играет важную роль в обеспечении цифровой безопасности, оно обладает рядом недостатков. Один из основных заключается в том, что, в случае компрометации ключа, преступнику также откроется доступ и к защищаемым сведениям.

Гомоморфное шифрование — это метод, при котором возможна обработка данных в зашифрованном виде. В работах [6, 7] отмечается возможность возникновения ошибок при выполнении операций над зашифрованными данными. В статьях указывается, что гомоморфное шифрование может оказаться неэффективным из-за ограничений на размер зашифрованных данных и количе-

ство операций, которые можно выполнить до того, как накопится достаточное количество ошибок, приводящих к невозможности получения правильного результата. Но, несмотря на это, гомоморфное шифрование является перспективной технологией для обработки зашифрованных данных в безопасной форме, хоть и на данный момент его использование ограничено и требует дополнительных исследований и усовершенствований [8].

Ещё одним подходом является нейросетевой преобразователь биометрия код (НПБК). В случае применения НПБК для защиты от подделки голоса можно использовать специальные звуковые фразы, которые должен произнести пользователь. Эти фразы должны быть тайными и не должны быть доступны злоумышленнику. Затем НПБК создаст уникальный код, который будет связан с ключом. В дальнейшем для аутентификации пользователя будет использоваться только ключ, а не биометрический образ [9].

Также для защиты биометрических данных могут быть применены нечёткие экстракторы. Нечёткие экстракторы основаны на квантовании «сырых» биометрических данных или вектора биометрических признаков и применении кодов, исправляющих ошибки, для корректировки нестабильных разрядов в бинарном представлении биометрического образа [10].

Для удобства сравнения двух подходов к биометрической аутентификации представлена табл. 1.

Таблица. 1

Сравнительная таблица технологий биометрической защиты

Критерии	Нечеткий экстрактор	НПБК
Алгоритм	Использует методы теории информации (квантование и помехоустойчивое кодирование)	Использует нейросетевые модели для преобразования биометрических параметров
Шифрование биометрических параметров	Не использует шифрование	Может сочетаться с классическим шифрованием, что позволяет получить эффект гомоморфного
Наличие угрозы от атак подмены или воспроизведения	Подвержен	Защищен
Производительность	Относительно медленный в процессе вычислений	Быстрый в процессе вычислений
Стандартизация	Нет	Семейство ГОСТ Р 52633
Точность распознавания	Низкая [11]	Средняя [12]
Объем обучающих данных	Малый	Малый
Длина ключа	Низкая [11]	Средняя [12]

Таким образом, можно сделать вывод о том, что НПБК обеспечивает более высокий уровень безопасности по сравнению с нечетким экстрактором, чему во многом способствует возможность генерации более длинных ключей и меньшая вероятность ошибок. Также он даёт лучшую производительность в процессе вычислений [13].

Состязательные атаки на биометрические системы и методы противодействия

Состязательные атаки могут быть осуществлены путем изменения биометрических данных или добавления в них шума, что может привести к принятию ошибочного решения в процессе аутентификации. Злоумышленник ищет способ выявить множество малозаметных изменений во входные данные, которые приведут к некорректной работе классификатора. Эти измененные входные данные называются "состязательными примерами", которые практически невозможно отличить от оригинальных образов, что затрудняет их обнаружение человеком. Состязательные атаки могут быть серьезной проблемой для безопасности биометрических систем [14]. Для защиты от состязательных атак применяются такие методы, как состязательное обучение, проверка на аномальные выбросы значений признаков, многофакторная аутентификация [15].

Метод состязательного обучения модели заключается в том, чтобы создавать искусственно сконструированные входные данные, которые намеренно вводятся в систему для проверки её устойчивости к состязательным атакам. Подобные образы называются состязательными примерами. Они позволяют оценить поведение модели в условиях, когда она подвергается намеренным изменениям входных данных. Если модель не может правильно классифицировать такой пример, то он используется для её обучения. Такой подход позволяет классификатору стать более устойчивым к состязательным атакам, поскольку он учится обрабатывать данные, специально сконструированные для его обмана [16].

Одним из наиболее актуальных типов угроз на системы автоматического распознавания диктора являются атаки, направленные на имитацию голоса целевого субъекта. По результатам, полученным в исследовании [17], было установлено, что наибольшую эффективность демонстрируют атаки с использованием дипфейковой речи. Для борьбы с ними, были представлены противодействующие меры, в которых применяются уникальные харак-

теристики человеческой речи, позволяющие распознать естественный голос от синтетического. Для выявления этих характеристик были использованы в качестве входных данных апериодические параметры (АП) и спектральная огибающая (СО) с функцией спектрограммы, что позволило добиться уровня ошибок $EER = 6,67$ и $t-DCF = 0,1604$ в сценарии с совместной задачей распознавания диктора по голосу и обнаружения образа, созданного при участии технологии дипфейк.

Способы противодействия дрейфу данных и концепций

Для надежной работы системы необходимо учитывать возможное появление дрейфов, которые можно классифицировать на два вида: дрейф данных и концепций. Согласно статье [18], дрейф данных отражает ситуацию, при которой статистические характеристики входных данных связаны, например, с условиями записи голоса, меняются со временем, что приводит к снижению производительности моделей машинного обучения, обученных на предыдущих данных. Дрейф концепций относится к изменениям в голосовых характеристиках диктора вследствие времени и других факторов. Это может быть вызвано физиологическими факторами, психоэмоциональным состоянием или другими внешними воздействиями. Для противодействия дрейфу концепций были разработаны методы адаптации модели, которые позволяют системе учитывать эти изменения.

Ключевым понятием, связанным с дрейфом является надежность — это способность системы сохранять требуемые характеристики и функциональность в течение заданного времени или при определенных условиях. Таким образом, дрейф снижает надежность.

Для оценки надежности применяются разнообразные метрики, которые позволяют оценить эффективность работы системы. Одной из основных метрик является вероятность ложного положительного (FAR) и ложного отрицательного (FRR) результата. FAR показывает, насколько часто система неправильно принимает неавторизованного пользователя за авторизованного. FRR, в свою очередь, указывает на вероятность неправильного отклонения авторизованного пользователя системой. Кроме того, существуют и другие метрики, которые оценивают качество распознавания и устойчивость классификатора. Примеры таких величин приведены в табл. 2.

Показатели эффективности биометрических систем

Метрика	Описание
Accuracy (точность)	Доля правильных ответов модели. Вычисляется как сумма правильных ответов и правильных отказов, поделённая на общее число примеров.
UAR (невзвешенный средний отзыв)	Среднее значение полноты для всех классов без учета их численности в данных.
Recall (полнота)	Доля правильно распознанных положительных примеров (true positive) относительно общего числа положительных примеров (true positive + false negative).
Precision (точность)	Доля правильно распознанных положительных примеров относительно общего числа, которые модель определила как положительные (true positive + false positive).
FRR (коэффициент ложного отказа)	Измеряет долю случаев, когда система не распознала легитимного пользователя.
FAR (коэффициент ложного пропуска)	Измеряет долю случаев, когда система ошибочно приняла злоумышленника за легитимного пользователя.
EER (равный уровень ошибок)	Определяется путем выставления порогового значения, при котором FAR и FRR равны.
minDCF (минимальная функция стоимости обнаружения)	представляет оценку баланса между FAR и FRR, позволяя учитывать реальные затраты на ошибки при принятии решений.
CMC (Cumulative Matching Characteristic)	Отображает зависимость вероятности правильной идентификации от количества рассматриваемых голосовых образов

Изменение свойств голосовых данных и снижение надежности может возникать из-за нескольких причин, включая использование разных микрофонов или поломку оборудования. Методы обнаружения дрейфа позволяют определить моменты, когда происходит изменение свойств. Это может быть достигнуто с использованием различных статистических тестов, таких как тест Колмогорова-Смирнова [19, 20] или расстояние Кульбака-Лейблера [21]. Чтобы адаптировать систему к новым условиям записи голоса, были разработаны различные методы нормализации сигнала и многоканальной обработки. Одним из таких является модифицированный адаптивный фильтр Калмана Sage-Husa [22].

В контексте преодоления различий в громкости и спектральном составе записей, полученных с разных микрофонов, используется метод среднеквадратичной нормализации сигнала [23]. Данный метод способствует выравниванию громкости аудиофайлов, обеспечивая желаемый уровень амплитудных значений. Подобные методы позволяют устранить различия в громкости путем выравнивания уровней звуковых сигналов.

В работе [24] авторы предлагают концепцию ElStream, которая использует ансамблевое обучение для обнаружения дрейфа концепций путем объединения нескольких классификаторов в единый комитет, что повышает эффективность. Допущение голоса классификатора осуществляется

лишь в том случае, если точность его прогноза превышает установленный порог. Для принятия решения используется техника голосования большинства. Этот подход показал повышенную точность на различных наборах данных по сравнению с предыдущими исследованиями и обычными алгоритмами машинного обучения.

Один из методов адаптации модели, используемый для преодоления дрейфа концепций, включает использование динамических моделей. Динамические модели учитывают изменения в голосовом образе диктора с течением времени. Это достигается путем учета динамических параметров, таких как скорость изменения голосовых характеристик. Использование динамических моделей позволяет более гибко адаптировать систему к изменениям в голосовом образе диктора, повышая ее устойчивость к дрейфу.

Таким образом, в работе [25] был разработан метод адаптации к концептуальным дрейфам (EACD), который применяет два эволюционных алгоритма – Replicator Dynamics (RD) и генетический алгоритм (GA) – для адаптации к различным изменениям концепций в потоках данных. RD оптимизирует размеры классификации в ансамбле, повышая точность предсказаний и сокращая время восстановления при изменениях концепций. GA оптимизирует случайно выбранные подпространства для адаптации к изменениям концепции. Оба алгоритма работают совместно для динамического

набора классификационных типов, способного адаптироваться к изменениям в данных.

Для обнаружения дрейфа данных и концепций авторы [18] предлагают использовать метод главных компонент для изучения изменения дисперсии. Для борьбы с ним предлагается использовать онлайн обучение, которое динамически настраивает размеры скрытых слоев на основе механизма взвешивания Hedge, что позволяет модели постоянно учиться и адаптироваться к новым данным. Эксперименты, проведенные на реальном наборе данных в IoT, показали, что предложенное решение стабилизирует производительность обнаружения вторжений как на обучающих, так и на тестовых данных по сравнению со статической глубокой нейронной сетью (НС).

Другой подход к противодействию дрейфу концепций состоит в использовании множественных шаблонов. Этот метод предполагает наличие нескольких шаблонов, представляющих различные голосовые состояния. Они могут быть созданы во время регистрации пользователя и представлять различные физические или эмоциональные состояния диктора. При аутентификации голоса система сравнивает запись с соответствующими шаблонами, что позволяет учесть возможные изменения в голосе диктора и снизить влияние дрейфа концепций на результаты идентификации. Метод нашёл применение в задаче распознавания речи [26]. Авторы использовали несколько шаблонов для каждого слова, записанных в разных условиях, например, с разными скоростями, интонациями и т. д., что увеличило точность распознавания с 70 до 88 %.

Также для противодействия дрейфу концепций могут применяться методы статистической нормализации. Эти методы позволяют выравнивать голосовые характеристики записей, чтобы они соответствовали эталонным значениям, используемым в системе [27]. Например, нормализация может быть применена к частотным характеристикам голоса, чтобы выровнять их соответствие стандартным значениям. Это помогает уменьшить влияние изменений в голосе диктора на процесс идентификации и аутентификации. Для поддержания надежности системы применяются подходы к уменьшению помех в сигнале. Один из таких — многоканальная обработка. Этот подход основывается на использовании информации с нескольких микрофонов для повышения качества и устойчивости системы. Многоканальная обработка может включать методы шумоподавления, согла-

сованной фильтрации и объединения сигналов с разных каналов [28].

Существующие базы голосовых образов

VoxCeleb2 содержит более миллиона записей от более чем 6000 личностей. Записи включают различные языки и акценты, что делает ее ценной для разработки межъязыковых систем идентификации диктора. Записи отражают разнообразие произношения дикторов из разных регионов, что позволяет исследователям разрабатывать и оценивать системы идентификации диктора, которые способны распознавать варианты произношения [29].

TIMIT — база данных голосовых образов, разработанная совместно компаниями *Texas Instruments*, *SRI International* и Массачусетским технологическим институтом. Архив был собран и обработан с 1986 по 1992 г. с целью изучения и разработки в области распознавания речи и идентификации диктора. Она состоит из аудиозаписей фонем, произносимых дикторами на английском языке, с использованием 16-битной линейной с частотой дискретизации 16 кГц [30].

Набор данных *RedDots* для распознавания голоса состоит из записей речи, собранных от 100 испытуемых, запись речи которых осуществлялась еженедельно в течение года. Каждый доброволец записывал 24 предложения на каждой сессии, включая 22 повторяющихся и 2 свободных текстовых. Всего в наборе данных 124800 записей речи. Корпус был создан для исследования влияния феномена старения на распознавание голоса, а также для изучения моделирования между и внутри говорящих с короткими высказываниями. Набор данных был создан командой исследователей из университета *Nanyang Technological University* в Сингапуре [31].

В апреле 2022 года был опубликован архив проекта *Common Voice*. В него вошли аудиозаписи дикторов более чем на 90 языках. В данную партию набора данных было включено 14 973 часа подтвержденной речи от более чем ста тысяч добровольцев [32].

Ещё одним популярным архивом является *LibriSpeech*, который содержит более 1000 часов чтения англоязычных текстов. Каждая запись предоставлена в формате 16-битного линейного кодека с частотой дискретизации 16 кГц и суммарный объем базы превышает 58 Гб. Информация об архивах голосовых образов представлена на табл. 3.

Сравнительная характеристика баз данных для распознавания речи

Название	Количество записей / участников	Количество часов	Языки	Формат записей	Средняя длина записи, секунд
VoxCeleb2	>1000000 записей, >6000 участников	> 2000	Многоязычный	16 бит, 16 кГц	7,8
TIMIT	6300 записей, 630 участников	4	8 диалектов английского	16 бит, 16 кГц	8,2
RedDots	124 800 записей, 100 участников	Не указано	Не указано	16 бит, 8 кГц	3
Common Voice	> 100 000 участников	14 973	93 языка	16 бит, 44,1 кГц	5
LibriSpeech	Не указано	> 1000	Английский	16 бит, 16 кГц	12 для обучения, 54 для теста
NIST SRE	>2000 участников. Постоянно увеличивается.	> 64	Многоязычный	16 бит, 16 кГц	10-60

Достигнутые результаты с учетом проводившихся оценок робастности

С зарождением идеи распознавания человека по голосу в середине XX в. исследователи сталкивались с ограниченными вычислительными ресурсами и методами, что влияло на точность разрабатываемых систем. В 1962 г. возникла концепция сопоставления голосовых спектрограмм, однако данную задачу приходилось решать вручную, с привлечением людей [33]. Они предварительно изучили свойства спектрограмм голосовых образцов, записанных группой людей, после чего соотносили выдаваемые им изображения только в рамках этой группы. Данные эксперименты продемонстрировали эффективность использования спектрограмм в качестве идентифицирующей формы представления голоса.

Расширение вычислительных возможностей в 1980-х позволило применить статистические и методы машинного обучения. Точность распознавания разрабатываемых методов достигала 54—95 % [34]. В 1990-х и 2000-х г. акцент сместился на эмоциональную и когнитивную голосовую аналитику, стала актуальной задача защиты биометрических данных от несанкционированного доступа [11]. В последние десятилетия, развитие нейронных сетей и глубокого обучения принесло повышение точности и эффективности. Одновременно с увеличением качества распознавания, исследователи стали уделять больше внимания другим проблемам голосовой аналитики:

1. Использование коротких высказываний для проведения идентификации;
2. Борьба с шумом;
3. Диаризация нескольких говорящих;
4. Обеспечение конфиденциальности биомет-

рических данных диктора;

5. Изменчивость голосовых характеристик вследствие старения [25];

6. Изменчивость в зависимости от здоровья и психоэмоционального состояния;

7. Многообразие языков и диалектов в идентифицирующей речи;

8. Эффективное текстонезависимое распознавание;

9. Различие устройств записи [22];

10. Атаки подделки голоса.

Существует несколько значимых подходов к извлечению векторных представлений: *x*-, *i*- и *d*-вектора. *i*-vector был представлен в 2011 г., его применение основывается на гауссовской смеси в то время, как *x*-vector, представленный в 2015 г., опирается на глубокие НС. *d*-vector также использует глубокие сети, его особенность заключается в уделяемом внимании динамическим аспектам речи. *d*-векторы учитывают последовательности звуковых фреймов. Этот метод позволяет извлечь вектор признаков с большей чувствительностью к изменениям в произнесении и интонации голоса. Многие научные работы посвящены экспериментальному сравнению этих подходов и пришли к выводу, что *i*-vector позволяет создавать менее ресурсоёмкие системы в то время, как *x*-vector обеспечивает более высокую эффективность благодаря глубокому анализу, что подтверждают результаты: 5,71 % против 9,23 % *EER* при использовании вероятностного линейного дискриминантного анализа (*PLDA*) в качестве классификатора [35]. Для оценки точности были привлечены базы *VoxCeleb*, *SWBD* и *NIST SRE* 2016.

Исходя из того, что потенциальные пользователи систем распознавания по голосу предпочитают короткие высказывания для аутентификации,

вскрывается проблема ограниченности фонетической информации в коротких речевых отрезках. В ответ на этот вызов исследователи [36] предложили метод его преодоления. Согласно проведённой работе выявлено, что извлечение вектора признаков при уменьшенных 6 и 7 слоях НС демонстрирует относительное уменьшение *EER* на 14 % до значения 13,35 % по сравнению с базовым методом (15,57 %) в условиях коротких пятисекундных высказываний взятых из *NIST2010*, из чего был сделан вывод о более успешной применимости малоразмерных слоёв для недлинных записей.

Основополагающий вклад в прогресс глубокого обучения и решения задачи эффективного распознавания диктора по речевым характеристикам внесла разработка архитектуры *ResNet*. Концепция *ResNet* заключается в использовании "остаточных блоков", которые включают дополнительные пропускающие связи между слоями. Это дает возможность пропускать один или несколько слоев внутри блока и передавать информацию напрямую от входа к выходу. Такой подход решает проблему затухания градиента, упрощает обучение сети, и позволяет эффективно обучать сеть на глубоких слоях. Авторы публикации [37] тестировали два варианта моделей на основе 34-слойной архитектуры *ResNet* с применением таких функций потерь как *AM-Softmax* и *AAM-Softmax*. В ходе экспериментов они добились значительного сокращения ошибок по сравнению с большинством работ *VoxSRC* на *Interspeech 2020* без применения комитетов нескольких классификаторов или постобработки. На тестовом наборе данных *VoxSRC 2020*, лучшая модель достигла *EER* = 5,19 % и *MinDCF* = 0,314.

В статье [38] рассматриваются два метода улучшения эффективности распознавания говорящего – улучшение речи и улучшение звука. Авторы проводят множественные эксперименты используя и сравнивая: *i* и *x* векторы, стробируемую свёрточную рекуррентную сеть (*GCRN*) и НС с долгой краткосрочной памятью (*LSTM*), Мелкепстральные коэффициенты (*MFCC*) и Гамматон-частотные кепстральные коэффициенты (*GFCC*), а

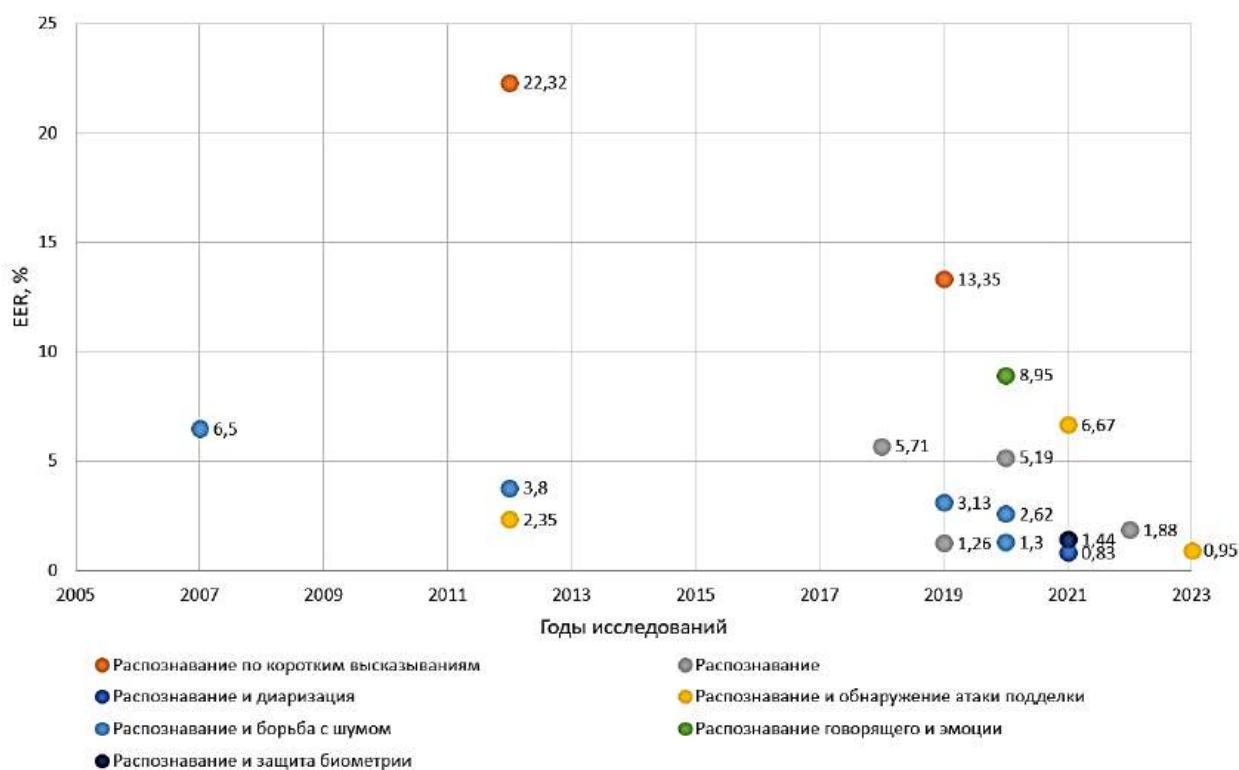
также испытывают формирователь луча с минимальной дисперсией без искажений (*MVDR*). Метод улучшения речи основан на использовании глубоких НС для извлечения характеристик голоса. Он показал значительное повышение эффективности по сравнению с классическим *i-vector*. Метод улучшения звука основан на использовании многоканального улучшения речи с помощью формирователя луча *MVDR*. Данный подход также продемонстрировал значительное повышение точности в сравнении с *x*-вектором. Авторы пришли к выводам о более высокой производительности в использовании *x*-векторов относительно *i*-векторов для всех проведённых экспериментов. Помимо данного вывода, была доказана высокая эффективность использования *GCRN* в ситуациях с высоким соотношением сигнал/шум (0—10 дБ).

Помимо задач идентификации и верификации личности диктора также существует более сложная задача разделения голосов на записи. Диаризация представляет собой автоматизированный процесс, направленный на сегментацию и идентификацию индивидуальных речевых источников в аудио или видеоматериалах. Результатом процедуры является информация о распределении субъектов по временным отрезкам записи, которая играет важную роль в последующей процедуре распознавания. В исследовании [39] представлена система диаризации, состоящая из компонентов: для извлечения векторов признаков, разделения речи и алгоритма *DOVER* для слияния результатов. Также были применены методы глубокого обучения, такие как *Res2Net* и *Conformer*, для повышения эффективности. Приведённая архитектура позволила достигнуть высокой точности *DER* = 6,23% на корпусе речи *VoxSRC Challenge 2020*. Для задачи верификации диктора командой исследователей была использована 50-слойная структура *Res2Net* с применением функции *AM-Softmax*. Лучшая модель, обученная на *VoxCeleb*, достигла значений *EER* = 0,83 % и *MinDCF* = 0,0473.

Для удобной иллюстрации основных полученных значений, достигнутых исследователями, были составлены табл. 4 и рисунок.

**Сравнительная таблица достигнутых результатов
в задаче распознавания диктора по голосовым характеристикам**

Применяемые методы	EER, %	Min_D CF	Используемая база	Год	Задача
<i>x-vector</i> + <i>PLDA</i> + расширение данных [35]	5,71		<i>VoxCeleb</i> , <i>SWBD</i> и <i>NIST SRE 2016</i>	2018	Распознавание
<i>x-vector</i> с уменьшенными 6 и 7 слоями + глубокие НС + расширение данных [36]	13,35		<i>NIST2010</i>	2019	Распознавание по коротким высказываниям
<i>ResNet</i> + <i>AAM-Softmax</i> [37]	5,19	0,314	<i>VoxSRC 2020</i>	2020	Распознавание
Извлечение признаков + разделение речи + <i>DOVER</i> + <i>Res2Net-50</i> + <i>AM-Softmax</i> [39]	0,83	0,0473	<i>VoxCeleb</i>	2021	Распознавание и диаризация
Объединение 4 топологий свёрточных НС (<i>ResNet</i>) + <i>PLDA</i> [40]	1,26		<i>VoxCeleb</i>	2019	Распознавание
<i>x-vector</i> + <i>GFCC</i> + многоканальное взвешенное предсказание + <i>MVDR</i> + <i>GCRN</i> [38]	2,62		<i>NIST SRE 2010</i>	2020	Распознавание и борьба с шумом
<i>АП</i> + <i>CO</i> + спектрограмма [17]	6,67	$t\text{-DCF} = 0,1604$	<i>ASVspoof 2019</i>	2021	Распознавание и обнаружение атаки подделки
<i>x-vector</i> + <i>ResNet</i> [41]	8,95—18,15		<i>MSP-Podcast</i>	2020	Распознавание говорящего и эмоции
<i>Thin ResNet-34</i> + <i>Softmax</i> [42]	3,13		<i>VoxCeleb2</i>	2019	Распознавание и борьба с шумом
спектр и логарифмический спектр + <i>LSTM-RNN</i> [43]	1,3		<i>Chinese Mandarin Corpus</i>	2020	Распознавание и борьба с шумом
предварительно обученная речевая модель <i>Wav2Vec2</i> + fine-tuning [44]	1,88		<i>Voxceleb1</i>	2022	Распознавание говорящего
<i>i-vector</i> + Гауссовский <i>PLDA</i> [45]	22,32	0,0849	<i>NIST SRE 2008</i>	2012	Распознавание по коротким высказываниям
<i>SpoTNet</i> + <i>CO</i> [46]	0,95		Нет данных	2023	Распознавание и обнаружение атаки подделки
Автокодировщик + НПКБ + ансамблирование [12]	1,44		Собственная	2021	Распознавание и защита биометрии



**Рис. 1. Иллюстрация распределения задач в распознавании диктора
и их результатов в зависимости от года исследования**

Исходя из полученного графика можно обнаружить, что задача распознавания диктора по коротким высказываниям (5 секунд) ещё недостаточно проработана, а также заметить тенденцию на снижение *EER* в зависимости от года публикации работ по каждой из указанных задач, что говорит о том, что наука движется в верном направлении и пройденные годы прошли не зря.

Заключение

Вектор развития речевых технологий и голосовой биометрии неоднократно менял своё направление. Наиболее широко представленной в литературе проблемой, с которой активно борются исследователи на протяжении более 3 десятилетий, оказалась борьба с шумом и низким качеством записанного аудиосигнала. Многие исследователи в рамках решения данной задачи проводили объединение нескольких корпусов данных содержащих, как чистую запись голосовых образов, так и файлы, содержащие шум. Соединение корпусов проходило с разным соотношением сигнал/шум, что позволяло изучать сразу множество условий. Наилучший результат $EER = 1,3\%$ был продемонстрирован учёными, применившими LSTM-RNN на логарифмическом спектре речевой записи.

Помимо данной проблемы, активно разрабатываются методы борьбы с другими аспектами, такими как дрейф голосовых характеристик, составительские атаки, спуфинг, а также задачи диаризации, защиты биометрических образов, распознавание эмоций и психологического настроения человека. Прогресс в этих областях открывает новые горизонты, благодаря использованию глубокого обучения и инновационных подходов. Различными исследовательскими группами были подготовлены свои архивы данных либо модифицированы существующие, которые были использованы для обучения и тестирования разработанных ими систем. К сожалению, далеко не каждый подобный архив выложен в открытый доступ и у большинства других учёных нет возможности протестировать свои подходы, сравнив полученные результаты с исходными.

Исходя из анализа проведённых научных работ, было подмечено отсутствие широкой апробации такого метода защиты биометрических шаблонов как НПБК на открытых источниках данных. Считаем, что перспективным направлением дальнейших исследований будет реализация различных архитектур, включающих в себя использование НПБК, обученных на общедоступных архивах. Также в ходе нашего обзора было выявлено отсут-

ствие в проводимых исследованиях решения сразу нескольких задач/проблем из чего следует необходимость создания подхода, который учитывает совокупность возможных видов атак. На данный момент не существует универсальной базы данных, удовлетворяющей всем требованиям практики. Такие базы данных должны включать в себя разнообразные голосовые данные, а также обеспечивать возможность использовать их в задачах защиты от различных видов атак, дрейфов и шума.

Исследование выполнено при финансовой поддержке Минцифры России (грант ИБ), проект № 40469-15/2022-к.

Литература

1. Just AI. Исследование. Рынок разговорного ИИ в России 2020-2025 [Электронный ресурс]. <https://just-ai.com/blog/issledovanie-rynok-razgovornogo-ii-v-rossii-2020-2025> (дата обращения: 12.04.2023).
2. IBM Security. Cost of a Data Breach Report 2020 [Электронный ресурс]. Режим доступа: <https://www.ibm.com/reports/data-breach-action-guide>. Дата обращения: 24.07.2023.
3. Калашников А. О. и др. Влияние новых технологий на информационную безопасность критической информационной инфраструктуры // Информация и безопасность. 2019. Т. 22. № 2. С. 156—169.
4. Наталья Касперская: никаких особых способов защиты биометрии нет // РИА Новости URL: <https://ria.ru/20211006/kasperskaya-1753227872.html> (дата обращения: 28.03.2023).
5. Сердюк В. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий. – Litres, 2022.
6. What is homomorphic encryption, and why isn't it mainstream? // keyfactor URL: <https://www.keyfactor.com/blog/what-is-homomorphic-encryption/> (дата обращения: 28.03.2023).
7. What is homomorphic encryption? // OpenMined URL: <https://blog.openmined.org/what-is-homomorphic-encryption/> (дата обращения: 28.03.2023).
8. Ложников П. С., Сулаво А. Е. Защищенное исполнение нейросетевых алгоритмов искусственного интеллекта: актуальность проблемы и перспективные решения // Региональная информатика и информационная безопасность. 2021. С. 104—108.
9. Сулаво А. Е. Биометрическая аутентификация на основе сети гиперболических нейронов байеса с трехуровневыми квантователями // Информационные технологии и автоматизация управления. 2020. С. 199—206.
10. Кузнецов А. А., Сергиенко Р. В., Уварова А. А. Нечеткий экстрактор на помехоустойчивых кодах для биометрической криптографии // Radiotekhnika. 2018. № 195. С. 224—234.
11. Monroe F. et al. Cryptographic key generation from voice // Proceedings 2001 IEEE Symposium on Security and Privacy. S&P 2001. IEEE, 2000. С. 202—213.
12. Сулаво А. Е., Иниватов Д. П., Стадников Д. Г., Чобан А. Г. Преобразователь образов голосовых паролей дикторов в криптографический ключ на основе комитета предварительно обученных сверточных нейронных сетей // Вопросы защиты информации. 2021. № 4. С. 23—33.

13. Иванов А. И., Ложников П. С., Сулаво А. Е. Оценка надежности верификации автографа на основе искусственных нейронных сетей, сетей многомерных функционалов Байеса и сетей квадратичных форм // Компьютерная оптика. 2017. Т. 41. № 5. С. 765—774.
14. Namiot D. Schemes of attacks on machine learning models // International Journal of Open Information Technologies. 2023. Т. 11. № 5. С. 68—86.
15. Лапина Т. И., Лапин Д. В. Многофакторная аутентификация пользователей информационных ресурсов // Информационно-измерительные и управляющие системы. 2017. Т. 15. № 5. С. 37—42.
16. Юнусов Н. Т., Смирнов С. В., Сакулин С. А. Состязательные примеры в задаче классификации изображений // Социально-экономическое управление: теория и практика. — 2019. № 4. С. 74—77.
17. Gao Y. et al. Detection and evaluation of human and machine generated speech in spoofing attacks on automatic speaker verification systems // 2021 IEEE Spoken Language Technology Workshop (SLT). IEEE, 2021. С. 544—551.
18. Wahab O. A. Intrusion detection in the iot under data and concept drifts: Online deep learning approach // IEEE Internet of Things Journal. 2022. Т. 9. № 20. С. 19706—19716.
19. Namiot D., Ilyushin E. Data shift monitoring in machine learning models // International Journal of Open Information Technologies. 2022. Т. 10. № 12. С. 84—93.
20. Кормилицин А. А., Калинина С. А., Меркулова А. Г. Исследование спектральных характеристик голоса человека в процессе профессиональной деятельности // Биотехнические, медицинские и экологические системы, измерительные устройства и робототехнические комплексы-Биомедсистемы-2022. 2022. С. 325—328.
21. Jabari S. et al. Multispectral change detection using multivariate Kullback-Leibler distance // ISPRS Journal of Photogrammetry and Remote sensing. 2019. Т. 147. С. 163—177.
22. Narasimhappa M. et al. MEMS-based IMU drift minimization: Sage Husa adaptive robust Kalman filtering // IEEE Sensors Journal. 2019. Т. 20. № 1. С. 250—260.
23. Sharma S., Tiwari G. SPEECH SENTIMENT ANALYSIS. // International Research Journal of Modernization in Engineering Technology and Science. 2023. №5. С. 9715—9722.
24. Abbasi A. et al. ElStream: An ensemble learning approach for concept drift detection in dynamic social big data stream learning // IEEE Access. 2021. Т. 9. С. 66408—66419.
25. Ghomeshi H., Gaber M. M., Kovalchuk Y. EACD: evolutionary adaptation to concept drifts in data streams // Data mining and knowledge discovery. 2019. Т. 33. С. 663—694.
26. Talbot M. Adapting to the speaker in automatic speech recognition // International journal of man-machine studies. — 1987. Т. 27. №. 4. С. 449—457.
27. Садыхов Р. Х., Ракуш В. В. Модели гауссовых смесей для верификации диктора по произвольной речи // Доклады Белорусского государственного университета информатики и радиоэлектроники. 2003. № 4 (4). С. 95—103.
28. Song S. et al. An integrated multi-channel approach for joint noise reduction and dereverberation // Applied Acoustics. — 2021. Т. 171. С. 107526.
29. Chung J. S., Nagrani A., Zisserman A. Voxceleb2: Deep speaker recognition // arXiv preprint arXiv:1806.05622, 2018.
30. Garofolo J. S. et al. DARPA TIMIT acoustic-phonetic continuous speech corpus CD-ROM. NIST speech disc 1-1.1 // NASA STI/Recon technical report n. 1993. Т. 93. С. 27403.
31. Lee K. A. et al. The RedDots data collection for speaker recognition // Interspeech 2015. 2015.
32. Ardila R., Branson M., Davis K. et al. Common voice: A massively-multilingual speech corpus // arXiv preprint arXiv:1912.06670. 2019.
33. Kersta L. G. Voiceprint identification // The Journal of the Acoustical Society of America. 1962. Т. 34. № 5_Supplement. С. 725—725.
34. Wohlford R., Wrench E., Landell B. A comparison of four techniques for automatic speaker recognition // ICASSP'80. IEEE International Conference on Acoustics, Speech, and Signal Processing. IEEE, 1980. Т. 5. С. 908—911.
35. Snyder D. et al. X-vectors: Robust dnn embeddings for speaker recognition // 2018 IEEE international conference on acoustics, speech and signal processing (ICASSP). IEEE, 2018. С. 5329—5333.
36. Kanagasundaram A. et al. A study of x-vector based speaker recognition on short utterances // Proceedings of the 20th Annual Conference of the International Speech Communication Association, INTERSPEECH 2019. Vol. 2019-September. ISCA (International Speech Communication Association), 2019. С. 2943—2947.
37. Heo H. S. et al. Clova baseline system for the voxceleb speaker recognition challenge 2020 // arXiv preprint arXiv:2009.14153. 2020.
38. Taherian H. et al. Robust speaker recognition based on single-channel and multi-channel speech enhancement // IEEE/ACM Transactions on Audio, Speech, and Language Processing. 2020. Т. 28. С. 1293—1302.
39. Xiao X. et al. Microsoft speaker diarization system for the voxceleb speaker recognition challenge 2020 // ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2021. С. 5824—5828.
40. Zeinali H. et al. But system description to voxceleb speaker recognition challenge 2019 // arXiv preprint arXiv:1910.12592. 2019.
41. Pappagari R. et al. x-vectors meet emotions: A study on dependencies between emotion and speaker recognition // ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2020. С. 7169—7173.
42. Xie W., Nagrani A., Chung J. S., Zisserman A. Utterance-level aggregation for speaker recognition in the wild // ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2019. С. 5791—5795.
43. El-Moneim S. A. et al. Text-independent speaker recognition using LSTM-RNN and speech enhancement // Multimedia Tools and Applications. 2020. Т. 79. С. 24013—24028.
44. Vaessen N., Van Leeuwen D. A. Fine-tuning wav2vec2 for speaker recognition // ICASSP 2022-2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2022. С. 7967—7971.
45. Kanagasundaram A., Vogt R., Dean D., Sridharan S. PLDA based speaker recognition on short utterances // Proceedings of The Speaker and Language Recognition Workshop: Odyssey 2012. International Speech Communication Association, 2012. С. 28—33.
46. Khan A., Malik K. M. SpotNet: A spoofing-aware Transformer Network for Effective Synthetic Speech Detection // Proceedings of the 2nd ACM International Workshop on Multimedia AI against Disinformation. 2023. С. 10—18.
47. Lei Y. et al. Towards noise-robust speaker recognition using probabilistic linear discriminant analysis // 2012 IEEE international conference on acoustics, speech and signal processing (ICASSP). IEEE, 2012. С. 4253—4256.
48. Ming J. et al. Robust speaker recognition in noisy conditions // IEEE Transactions on Audio, Speech, and Language Processing. 2007. Т. 15. № 5. С. 1711—1723.
49. Wu Z., Chng E. S., Li H. Detecting converted speech and natural speech for anti-spoofing attack in speaker recognition // Thirteenth Annual Conference of the International Speech Communication Association. 2012.

Analytical study of the problem of biometric identification and authentication of subjects by voice

D. P. Inivatov

Omsk State Technical University, Omsk, Russia

This article presents an overview of modern achievements and methods in the field of human voice recognition and biometric identification. The key challenges faced by researchers in this field, such as the fight against noise, voice drift, spoofing, diarization, contention attacks, etc. are considered. Comparative tables of the results of research conducted in this area are given. Particular attention is paid to the progress in the development of methods that can improve the accuracy of voice recognition under conditions of noise and variable voice characteristics. As a result of the review, the best values for the studied tasks are given: diarization — EER = 0.83 %, noise control — 1.3 %, emotion recognition — 8.95 %. It is noted that a promising direction can be considered the implementation of various architectures, including a biometric-code neural network converter in order to protect biometric templates.

Keywords: automatic speaker recognition, deep learning, spoofing, anti-noise, speaker voice parameters, biometric authentication, voice data corpora.

Bibliography — 49 references.

Received September 5, 2023

ОБЩИЕ ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ОБЪЕКТОВ

УДК 519.873

DOI: 10.52190/2073-2600_2023_3_39

EDN: SHXMKG

Выбор оптимальной по точности контрольной аппаратуры для оценки эффективности защиты информации

А. П. Лапсарь, канд. техн. наук

Управление ФСТЭК России по Южному и Северо-Кавказскому федеральным округам,
г. Ростов-на-Дону, Россия

А. С. Любухин

Ростовский государственный экономический университет (РИНХ), г. Ростов-на-Дону, Россия

Рассмотрена задача выбора наиболее эффективной контрольной аппаратуры для оценки параметров защищенности объекта информатизации. В качестве решения предложено оптимизировать точность используемых в аппаратуре средств измерений при заданных вероятностях ложного и необнаруженного отказов.

Ключевые слова: контрольная аппаратура, защита информации, оптимальная погрешность, предел допускаемой погрешности, ошибка распознавания, ложный и необнаруженный отказы.

Современные условия диктуют повышенные требования к обеспечению информационной безопасности во всех областях жизни и деятельности государства. Целостность и конфиденциальность информации ограниченного распространения достигается созданием объектов информатизации, безопасность которых обеспечивается выполнением ряда установленных мероприятий в соответствии с заданными требованиями. При этом в сложившейся геополитической обстановке поставленные руководством страны задачи по импортозамещению и обеспечению технологического суверенитета страны распространяются и на средства контроля эффективности защиты информации [1—3].

Важнейшей процедурой подтверждения соответствия объектов защиты заданным требованиям по информационной безопасности является их аттестация. Аттестация объектов информатизации и предусмотренный в процессе эксплуатации контроль эффективности защиты информации предполагают использование контрольной аппаратуры,

предназначенной для измерения необходимых параметров, определенных программой и методиками испытаний. Требования к контрольной аппаратуре — это наборы контролируемых параметров, виды тестирующих сигналов, диапазоны измерений и другие характеристики.

Важнейшим элементом контрольной аппаратуры являются средства измерений контролируемых параметров. Можно констатировать, что качество контрольной аппаратуры во многом зависит от метрологических характеристик применяемых средств измерений, одной из которых является их точность, определяемая пределами допустимых погрешностей [4, 5]. От точности определения результатов зависит не только достоверность измерений, но и стоимость применяемой аппаратуры и расходы на ее содержание (поверка, техническое обслуживание и т. д.). При прочих равных условиях повышение точности контрольной аппаратуры (снижение погрешности средств измерений) приводит к повышению ее стоимости.

Проведение аттестационных испытаний и контроля эффективности с точки зрения теории надежности сводится к определению работоспособности объекта контроля. Известно, что работоспособность или пригодность объекта к дальнейшей эксплуатации определяется нахождением требуемых характеристик и параметров его функционирования в границах области допустимых

Лапсарь Алексей Петрович, доцент.

E-mail: lapsar1958@mail.ru

Любухин Алексей Сергеевич, аспирант.

E-mail: r.vv2020@mail.ru

Статья поступила в редакцию 25 июня 2023 г.

© Лапсарь А. П., Любухин А. С., 2023

значений (допусков) [6, 7]. В связи с этим ряд измерительных задач по подтверждению заявленных характеристик (первичная аттестация объектов информатизации, испытание новых изделий и средств защиты) можно условно отнести к категории исследовательских. При этом неизбежно возникновение ошибок 1-го и 2-го рода, особенно если характеристика (измеряемый параметр) находится на границе допустимой области. Величина ошибок и соответственно потери от их появления напрямую зависят от точностных характеристик используемой аппаратуры. Потери от ошибок 1-го рода с повышением точности возрастают, от ошибок 2-го рода — уменьшаются, стоимость же измерительной аппаратуры только возрастает [4, 6, 7].

Таким образом, налицо оптимизационная задача по обоснованию точности используемой контрольной аппаратуры, обеспечивающей, с одной стороны, минимальную стоимость ее эксплуатации, а с другой — приемлемые (допустимые) потери от возникновения ошибок 1-го и 2-го рода.

Цель работы — разработать метод выбора контрольной аппаратуры для оценки параметров защищенности объекта информатизации на основе оптимизации точности используемых средств измерений.

Постановка задачи

Не теряя общности, рассмотрим один отдельно взятый параметр, оцениваемый (измеряемый) в ходе контроля эффективности. В аппаратуре контроля используют цифровые измерители, преобразующие непрерывное значение измеряемого параметра в цифровую форму. Поступающий на вход измерительной аппаратуры аналоговый сигнал преобразуется в последовательный набор "ступенек", характеризующих его числовое значение, т. е. непрерывный параметр разбивается на некоторое число уровней N , размеры (величина) которых определяются точностью контрольной аппаратуры $N = X(t)/\Delta x(t)$, здесь $X(t)$ — ширина диапазона контрольной аппаратуры, $\Delta x(t)$ — ширина уровня, характеризующая ее точность, как правило $\Delta x(t) = 2\Delta(x)$, где $\Delta(x)$ — предел допускаемой погрешности аппаратуры.

На вход измерительной аппаратуры от контролируемого объекта поступает сигнал $S(x, t)$, имеющий N уровней $S(x, t) \in \{s_n(x_n, t)\}$, $n = \overline{2, N}$.

С точки зрения оценки соответствия контролируемого объекта заданным характеристикам

наиболее информативной является ситуация, когда оцениваемый параметр находится в окрестности границы области допустимых значений. Для достижения поставленной цели из множества N уровней сигнала выделим два, один из которых $s_{g-}(x, t)$ находится ниже границы x_g области допустимых значений (в зоне допусков), а другой $s_{g+}(x, t)$ — выше (за пределами допуска). Таким образом, оценка значения измеренного параметра как принадлежащего уровню $s_{g-}(x, t)$ свидетельствует об исправности контролируемого объекта (параметр в норме), а принадлежность уровню $s_{g+}(x, t)$ говорит о его неисправности (выход параметра за границы области допустимых значений). Известно, что на измеряемый сигнал оказывают влияние многочисленные непреднамеренные помехи. Это приводит к тому, что на вход контрольной аппаратуры будет поступать аддитивная смесь полезного сигнала (измеряемого параметра) и белого гауссовского шума $n(t)$: $x_{KA}(t) = x(t) + n(t)$ [4, 7, 8]. Результат измерения параметра контрольной аппаратурой также будет носить случайный характер. В соответствии с требованиями закона об обеспечении единства измерений результат измерения определяют следующим образом: $x_{KA}(t) = x(t) \pm \Delta(x)$, где $\Delta(x)$ — предел абсолютной допускаемой погрешности используемой контрольной аппаратуры.

Пусть измеряемый параметр находится вблизи области допустимых значений. Эффективность оценки уровня сигнала, то есть отнесения его к одному из уровней $s_{g-}(t)$ (параметр в норме), или $s_{g+}(x, t)$ (параметр не в норме), определяется вероятностью соответствующей ошибки. Вероятность ошибки 1-го рода, т. е. того, что сигнал, фактически находящийся в пределах границы области допустимых значений (в пределах уровня $s_{g-}(t)$), по результатам измерений будет отнесен к уровню $s_{g+}(t)$ допусков, будет равна

$$P_{\text{ЛЮ}}(x) = \int_x^{\infty} p(x_{g-}) dx. \text{ Соответственно вероятность}$$

ошибки 2-го рода, т. е. сигнал, фактически находящийся за пределами границы области допустимых значений $s_{g+}(t)$, по результатам измерений будет отнесен к уровню $s_{g-}(t)$, равна

$$P_{\text{НО}}(x) = \int_{-\infty}^x p(x_{g+}) dx, \text{ } p(x_i) \text{ — плотность распределения оцениваемого параметра.}$$

Контрольная аппаратура, используемая для измерений значений параметра, из-за собственной погрешности также может инициировать ошибки 1-го или 2-го рода. Вероятность ложного (ошибка 1-го рода) и необнаруженного (ошибка 2-го рода) отказа с учетом распределения погрешности измерителя контрольной аппаратуры

$$P_{КАg-}(x) = \int_{x_i}^{\infty} p(x_{g-}) dx \int_{x_i}^{\infty} p(y) dy \text{ и } P_{КАg+}(x) = \int_{x_i}^{\infty} p(x_{g+}) dx \int_{x_i}^{\infty} p(y) dy \text{ соответственно.}$$

С учетом $P_{КАg-}(x)$ и $P_{КАg+}(x)$ вероятности ошибочных решений (принятия одного уровня сигнала за другой) суммарные вероятности ошибок распознавания уровней сигнала будут соответственно равны $P_{\Sigma g-}(x) = P_{ЛО}(x) + P_{КАg-}(x)$ и $P_{\Sigma g+}(x) = P_{НО}(x) + P_{КАg+}(x)$. Тогда общая ошибка распознавания уровней сигнала будет характеризоваться вероятностью $P_{\Sigma}(x) = P_{\Sigma g-}(x) + P_{\Sigma g+}(x)$, а вероятность правильного распознавания — $P(x) = 1 - P_{\Sigma}(x)$.

Поскольку на оцениваемый параметр и контрольную аппаратуру действует большое число независимых случайных факторов, в соответствии с центральной предельной теоремой как исследуемый параметр, так и погрешность измерения распределяются по нормальному закону [9, 10]. Тогда

$$P_{\Sigma}(x) = \frac{1}{2\pi} \int_0^{\infty} \exp\left[-\frac{1}{2}\left(m_{xg-} - A_{xg-}^{-1}\right)\right]^2 dx_{g-} \times \int_{\alpha}^{\infty} \exp\left[-\frac{1}{2}\left(m_{xg+} - A_{xg+}^{-1}\right)\right]^2 dx_{g+}.$$

Здесь m_{xg-} и m_{xg+} — математические ожидания, A_{xg-} и A_{xg+} — коэффициенты вариации исследуемого сигнала на соответствующем уровне, $\alpha = [s_{g+}(x_{g+}, t)] [s_{g-}(x_{g-}, t)]^{-1}$.

Обоснование точности контрольной аппаратуры

На вход контрольной аппаратуры поступает реализация измерительного эксперимента, представляющая собой аддитивную смесь исследуемого полезного сигнала и внутренней помехи кон-

трольной аппаратуры $y(x, t) = S(x, t) + n(t)$. Задача определения уровня сигнала состоит в том, чтобы на основе анализа значения его реализации, полученного с использованием контрольной аппаратуры с известной точностью, принять обоснованное решение о нахождении сигнала в области допустимых значений $s_{g-}(t)$ или о выходе его за пределы допуска $s_{g+}(t)$, т. е. необходимо принять решение, к какому из двух соседних уровней принадлежит сигнал. Количественной мерой достоверности принятого решения служит величина, обратная вероятности принятия ошибочного решения. Вероятность ошибочного решения обусловлена тем, что исследуемый сигнал из-за внутренних шумов и искажений в измерительном канале контрольной аппаратуры придает реализации $y(x, t)$ случайный характер [5, 6, 11]. Это обстоятельство приводит к тому, что измеренное значение содержит погрешность, а оценка, принятая по результатам измерения его значения, является стохастической. В дальнейшем будем считать условные плотности $p_i(x|y)$ оценки измеряемого параметра унимодальными.

При условии, что число распознаваемых уровней априори известно, а также известны плотности распределения уровней сигнала на каждом из уровней, т. е. известны $p_{g-}(x|y)$ и $p_{g+}(x|y)$, задача различения сигнала $S(x, t)$ состоит в проверке истинности двух гипотез: Γ_1 — измеренное значение сигнала $x_{из}(t)$ принадлежит уровню $s_{g-}(t)$, и Γ_2 — уровню $s_{g+}(t)$.

Алгоритм выбора конкретной гипотезы предполагает сравнение измеренного значения $x_{из}(t)$ с пороговыми значениями каждого из уровней x_{0g-} и x_{0g+} . Для оценки используем следующее решающее правило: при $x_{0g-} \leq x_{из}(t) < x_{0g+}$ и $\sigma(x_{g-}) < \sigma(x_{g+})$ принимаем гипотезу Γ_1 , а для $\sigma(x_{g-}) > \sigma(x_{g+})$ — гипотезу Γ_2 . Соответственно при $x_{из}(t) \geq x_{0g+}$ и $\sigma(x_{g-}) < \sigma(x_{g+})$ принимаем гипотезу Γ_2 , а для $\sigma(x_{g-}) > \sigma(x_{g+})$ — гипотезу Γ_1 . Законы распределения плотности вероятности параметра на каждом из рассматриваемых уровней характеризуются соответствующими дисперсиями случайного распределения $D(x_{g-}) = \sigma^2(x_{g-})$ и $D(x_{g+}) = \sigma^2(x_{g+})$.

С использованием указанного алгоритма задача различения уровней сигнала характеризуется суммарной вероятностью принятия ошибочного решения $P_{\Sigma}(x) = P_{\text{ЛО}}(x) + P_{\text{НО}}(x)$, где

$$P_{\text{ЛО}}(x) = \begin{cases} \int_{-\infty}^{x_{g-}} p_{g-}(x|y)dy + \int_{x_{g+}}^{\infty} p_{g-}(x|y)dy, & \sigma(x_{g-}) < \sigma(x_{g+}), \\ \int_{x_{g-}}^{x_{g+}} p_{g-}(x|y)dy, & \sigma(x_{g-}) > \sigma(x_{g+}), \end{cases} \quad (1)$$

$$P_{\text{НО}}(x) = \begin{cases} \int_{x_{g-}}^{x_{g+}} p_{g+}(x|y)dy, & \sigma(x_{g-}) < \sigma(x_{g+}), \\ \int_{-\infty}^{x_{g-}} p_{g+}(x|y)dy + \int_{x_{g+}}^{\infty} p_{g+}(x|y)dy, & \sigma(x_{g-}) > \sigma(x_{g+}). \end{cases} \quad (2)$$

В соотношениях (1) и (2) приняты следующие обозначения: $P_{\text{ЛО}}(x)$ — вероятность того, что уровень $s_{g-}(t)$ будет идентифицирован как $s_{g+}(t)$ (ложный отказ), а $P_{\text{НО}}(x)$ — вероятность того, что уровень $s_{g+}(t)$ будет идентифицирован как $s_{g-}(t)$ (необнаруженный отказ). С учетом (1) и (2) $P_{\Sigma}(x)$ определяем одним из следующих выражений:

$$P_{\Sigma}(x_{0g-}, x_{0g+}) = \int_{x_{0g-}}^{x_{0g+}} p_{g+}(x|y)dy + \int_{-\infty}^{x_{0g-}} p_{g-}(x|y)dy + \int_{x_{0g+}}^{\infty} p_{g-}(x|y)dy, \quad \sigma(x_{g-}) < \sigma(x_{g+}), \quad (3)$$

$$P_{\Sigma}(x_{0g-}, x_{0g+}) = \int_{-\infty}^{x_{0g-}} p_{g+}(x|y)dy + \int_{x_{0g+}}^{\infty} p_{g+}(x|y)dy + \int_{x_{0g-}}^{x_{0g+}} p_{g-}(x|y)dy, \quad \sigma(x_{g-}) > \sigma(x_{g+}). \quad (4)$$

Из условия взаимно однозначной связи между ошибками оценки параметра $x_i(t)$ и вероятностью $P_{\Sigma}(x)$ становится возможным вычисление шага дискретизации $\Delta d = \hat{x}_{g+}(t) - \hat{x}_{g-}(t)$ при измерении контрольной аппаратурой параметра, используемого в задаче различения двух соседних

уровней сигнала $S(x, t)$. В свою очередь, шаг дискретизации определяет требуемую точность контрольной аппаратуры [4, 12].

Определим значения x_{0g-} и x_{0g+} , при которых обеспечивается минимум вероятности $P_{\Sigma}(x)$. Условием экстремума функции является равенство нулю ее первой производной. Для отыскания минимума продифференцируем (3) и (4) по пороговому значению параметра $x_i(t)$, $i = [0_{g-}, 0_{g+}]$ и приравняем нулю полученные выражения:

$$\frac{dP(x_{0g-}, x_{0g+})}{dx_{0g-}} = 0; \quad \frac{dP(x_{0g-}, x_{0g+})}{dx_{0g+}} = 0. \quad (5)$$

Соотношения (5) выполняются при следующих условиях:

$$p_{g-}(x_{0g-}) = p_{g+}(x_{0g+}), \quad p_{g+}(x_{0g+}) = p_{g-}(x_{0g-}), \quad \sigma(x_{g-}) < \sigma(x_{g+}); \quad (6)$$

$$p_{g+}(x_{0g+}) = p_{g-}(x_{0g-}), \quad p_{g-}(x_{0g-}) = p_{g+}(x_{0g+}), \quad \sigma(x_{g-}) > \sigma(x_{g+}). \quad (7)$$

Идентичность выражений (6) и (7) свидетельствует, что для случая неравноточных измерений исследуемого параметра оптимальное с точки зрения минимизации ошибок $P_{\Sigma}(x)$ значение пороговых уровней соответствует абсциссам точек пересечения условных плотностей распределения вероятностей измеряемого признака различаемых сигналов. Это позволяет получить аналитические зависимости, связывающие вероятность $P_{\Sigma 2}(x)$ с ошибками оценивания параметра $x_i(t)$, определяемыми, в свою очередь, точностными характеристиками контрольной аппаратуры.

Пример реализации полученных результатов

Проиллюстрируем полученные результаты на примере без привязки к конкретной физической величине. Считаем, что ошибка оценки (измерения) параметра $x_i(t)$ распределена по нормальному закону с дисперсией $D(x_i) = \sigma^2(x_i)$. С учетом этого запишем выражения для условных плотностей распределения

$$\begin{cases} p_{g-}(x|y) = \frac{1}{\sqrt{2\pi\sigma(x_{g-})}} \exp\left\{-\frac{(x-\hat{x}_{изг-})^2}{2\sigma^2(x_{g-})}\right\}, \\ p_{g+}(x|y) = \frac{1}{\sqrt{2\pi\sigma(x_{g+})}} \exp\left\{-\frac{(x-\hat{x}_{изг+})^2}{2\sigma^2(x_{g+})}\right\}, \end{cases} \quad (8)$$

где $\hat{x}_{изг-}$ и $\hat{x}_{изг+}$ — оценки измеряемого параметра, а $\sigma^2(x_{g-})$ и $\sigma^2(x_{g+})$ — дисперсии оценок измеряемого параметра соответствующего уровня. Тогда, с учетом (7) и (8),

$$\begin{aligned} \frac{1}{\sigma(x_{g-})} \exp\left\{-\frac{(x-x_{g-})^2}{2\sigma^2(x_{g-})}\right\} &= \\ &= \frac{1}{\sigma(x_{g+})} \exp\left\{-\frac{(x-x_{g+})^2}{2\sigma^2(x_{g+})}\right\}. \end{aligned} \quad (9)$$

Прологарифмировав (9) и решив полученное уравнение, относительно $x(t)$ получим оптимальные значения порогов x_{0g-} и x_{0g+} .

$$\begin{aligned} x_{0g-} &= \left[\sigma^2(x_{g-})\hat{x}_{изг+} - \sigma^2(x_{g+})\hat{x}_{изг-} + \lambda \right] \times \\ &\times \left[\sigma^2(x_{g-}) - \sigma^2(x_{g+}) \right]^{-1}, \\ x_{0g+} &= \left[\sigma^2(x_{g-})\hat{x}_{изг+} - \sigma^2(x_{g+})\hat{x}_{изг-} - \lambda \right] \times \\ &\times \left[\sigma^2(x_{g-}) - \sigma^2(x_{g+}) \right]^{-1}, \end{aligned} \quad (10)$$

где

$$\begin{aligned} \lambda &= \left\{ \left[\sigma^2(x_{g-})\hat{x}_{изг+} - \sigma^2(x_{g+})\hat{x}_{изг-} \right] - \right. \\ &\left. - \left[\sigma^2(x_{g-}) - \sigma^2(x_{g+}) \right] \right. \\ &\times \left. \left[\sigma^2(x_{g-})\hat{x}_{изг+}^2 - \sigma^2(x_{g+})\hat{x}_{изг-}^2 - \right. \right. \\ &\left. \left. - 2\sigma^2(x_{g+})\hat{x}_{изг+} \ln \left(\sigma^2(x_{g-}) \left[\sigma^2(x_{g+}) \right]^{1/2} \right) \right] \right\}^{1/2}. \end{aligned}$$

Подставив (10) в (3) и (4), с учетом (9), выражение для вероятности ошибки $P_{\Sigma}(x)$ запишется в следующем виде:

$$\begin{aligned} P_{\Sigma}(x) &= 1 + \Phi \left[\frac{x_{0g+} - \hat{x}_{изг+}}{\sigma(x_{g+})} \right] - \Phi \left[\frac{x_{0g-} - \hat{x}_{изг+}}{\sigma(x_{g+})} \right] + \\ &+ \Phi \left[\frac{x_{0g-} - \hat{x}_{изг-}}{\sigma(x_{g-})} \right] - \Phi \left[\frac{x_{0g+} - \hat{x}_{изг-}}{\sigma(x_{g-})} \right], \\ &\forall \sigma(x_{g-}) < \sigma(x_{g+}), \end{aligned} \quad (11)$$

$$\begin{aligned} P_{\Sigma}(x) &= 1 + \Phi \left[\frac{x_{0g+} - \hat{x}_{изг+}}{\sigma(x_{g+})} \right] - \Phi \left[\frac{x_{0g+} - \hat{x}_{изг+}}{\sigma(x_{g+})} \right] + \\ &+ \Phi \left[\frac{x_{0g+} - \hat{x}_{изг-}}{\sigma(x_{g-})} \right] - \Phi \left[\frac{x_{0g-} - \hat{x}_{изг-}}{\sigma(x_{g-})} \right], \\ &\forall \sigma(x_{g-}) > \sigma(x_{g+}), \end{aligned} \quad (12)$$

где $\Phi[\cdot]$ — табличный интеграл вероятностей [12, 13].

Приведенные выражения для вероятности ошибки $P_{\Sigma}(x)$ служат основой для вычисления оптимальной погрешности контрольной аппаратуры, поскольку предел допускаемой погрешности цифрового средства измерений и его шаг дискретизации на каждом диапазоне связаны однозначной линейной зависимостью.

На рис. 1 приведены семейства зависимостей $P_{\Sigma} = F_1[\sigma(x)]$, рассчитанные по представленным формулам при различных значениях шага дискретизации $\Delta d = x_{g+}(t) - x_{g-}(t)$, P_{Σ} . Анализ представленных графиков показывает, что реализация предлагаемого подхода позволяет априори определить требования к точности оценки параметра $x_i(t)$, при которой обеспечивается заданное качество различения уровней сигнала $s_{g-}(x, t)$ и $s_{g+}(x, t)$ на основе минимизации ошибок 1-го и 2-го рода.

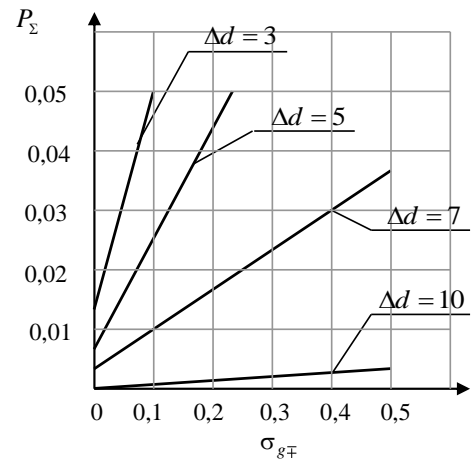


Рис. 1. Семейства зависимостей $P_{\Sigma} = F_1[\sigma(x)]$

Из соотношений (11) и (12) следует, что $\sigma(x_{g-}) = F_2[\sigma(x_{g+})]$ вычисляется во всех точках, кроме точки $\sigma(x_{g-}) = \sigma(x_{g+})$, которая соответствует равноточным измерениям параметра $x_i(t)$.

Такая ситуация наиболее характерна для практики, поэтому рассмотрим эту точку более подробно. При $\sigma(x_{g-}) = \sigma(x_{g+})$ значения унимодальных условных плотностей распределения вероятности $p_i(x|y)$ пересекаются в одной точке, т. е.

$$P_{HO}(x) = \int_{-\infty}^{x_0} p_{g+}(x|y) dy, \quad P_{ЛО}(x) = \int_{x_0}^{\infty} p_{g-}(x|y) dy, \quad \text{а}$$

суммарная вероятность ошибки:

$$P_{\Sigma}(x_0) = \int_{-\infty}^{x_0} p_{g+}(x|y) dy + \int_{x_0}^{\infty} p_{g-}(x|y) dy. \quad (13)$$

Продифференцировав (13) по x_0 и приравняв результат нулю, получим соотношение $p_{g-}(x|y) = p_{g+}(x|y)$, что полностью согласуется с физическим смыслом процесса измерения. Под-

ставив (8) в (13), получим $x_0 = \frac{1}{2}[\hat{x}_{изг-} + \hat{x}_{изг+}]$ и

$$P_{\Sigma 2} = 2 - 2\Phi\left\{\left[\hat{x}_{изг+} + \hat{x}_{изг-}\right](2\sigma_0)^{-1}\right\}. \quad \text{Таким обра-}$$

зом, полученные результаты показывают, что оптимальное значение погрешности контрольной аппаратуры равно

$$\sigma_{\text{опт}} = \left[\hat{x}_{изг+} - \hat{x}_{изг-}\right] \left[2\Phi^{-1}\right] \left(1 - \frac{1}{2}P_{\Sigma}\right). \quad (14)$$

На рис. 2 представлены семейства зависимостей $\sigma_{\text{опт}} = F[P_{\Sigma}(x)]$ при различных значениях шага дискретизации $\Delta d = \hat{x}_{изг+} - \hat{x}_{изг-}$. Они характеризуют оптимальные значения точности оценки параметра $x_i(t)$, используемого в качестве признака при решении задачи различения уровней сигнала. Полученные результаты позволяют на базе априори установленных величин вероятностей ошибок оценки параметра выбрать контрольную аппаратуру с соответствующей погрешностью.

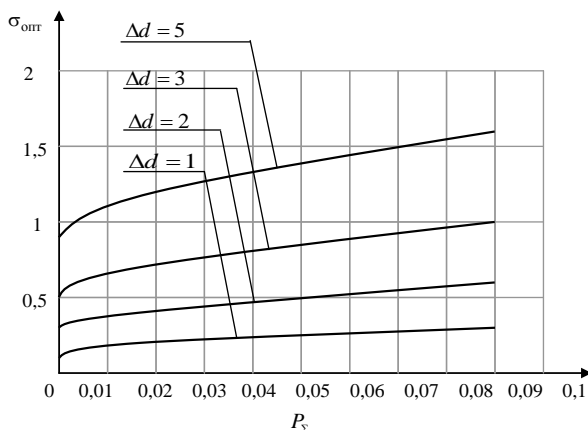


Рис. 2. Семейства зависимостей $\sigma_{\text{опт}} = F[P_{\Sigma}(x)]$

Заключение

Предложено решение задачи выбора контрольной аппаратуры для оценки параметров защищенности объекта информатизации на базе оптимизации точности используемых средств измерений при заданных вероятностях ошибок 1-го и 2-го рода. На базе априори заданного максимально допустимого значения ошибки измерения информативного параметра и решения (14), вычисляем требуемые характеристики контрольной аппаратуры по критерию "точность".

Предложенный подход может быть применен при создании и последующих испытаниях на подтверждение соответствия контрольной аппаратуры заявленным требованиям при ее сертификации. При этом экономическая целесообразность разработки или закупки контрольной аппаратуры позволяет оптимизировать расходы на обеспечение процессов оценки защищенности объектов информатизации. Таким образом, результаты данного исследования позволяют более эффективно использовать ресурсы, направляемые на обеспечение решения вопросов информационной безопасности и технологического суверенитета страны.

Литература

1. Послание Президента Федеральному Собранию [Электронный ресурс]. Режим доступа: <http://kremlin.ru/events/president/news/70565>.
2. Любухин А. С. Критическая информационная инфраструктура Российской Федерации в условиях санкций и импортозамещения // Научный альманах Центрального Черноземья. 2022. № 1-5. С. 110—115.
3. Отчет Positive Technologies [Электронный ресурс]. Режим доступа: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q2/>.
4. Воробьев С. Н. Цифровая обработка сигналов. — М.: Академия, 2013. — 320 с.
5. Френкс Л. Теория сигналов / пер. с англ. Краевской М. Р., Седлецкого Р. М. / под ред. Вакмана Д. Е. — М.: Советское радио, 1974. — 343 с.
6. Яхьяев Н. Я., Короблин А. В. Основы теории надежности: учебник для студентов Учр. высш. проф. образования. Изд. 2, перераб. — М.: Издательский центр "Академия", 2014. — 208 с.
7. Острейковский В. А. Теория надежности. — М.: Высшая школа, 2003. — 462 с.
8. Ку Х. Н. Влияние аддитивного белого гауссовского шума на спектральную плотность QPSK: сб. тез. докладов 56-й науч. конф. аспирантов, магистрантов и студентов "Радиотехника и электроника". — Минск, 2020. С. 169—170.
9. Гринь А. Г. О центральной предельной теореме для симметричных функций от зависимых величин // Математические структуры и моделирование. 2017. № 1(41). С. 5—11.
10. Булинский А. В. Центральная предельная теорема для положительно ассоциированных стационарных случайных полей // Вестник Санкт-Петербургского университета. Математика. Механика. Астрономия. 2011. № 2. С. 5—13.

11. Кремер Н. Ш. Теория вероятностей и математическая статистика: учеб. и практикум для вузов. Изд. 5, перераб. и доп. — М.: Издательство Юрайт, 2023. — 538 с.

12. Матальцкий М. А., Хацкевич Г. А. Теория вероятностей, математическая статистика и случайные процессы: учеб. пособие для студентов учреждений высшего образования по

физико-математическим специальностям. — Минск: Вышэйшая школа, 2012. — 719 с.

13. Вентцель Е. С., Овчаров Л. А. Теория случайных процессов и ее инженерные приложения. — М.: Издательский центр "Академия", 2003. — 429 с.

Selection of control equipment optimal in terms of accuracy for evaluating the effectiveness of information protection

A. P. Lapsar

Office of the FSTEC of Russia for the Southern and North Caucasian Federal Districts,
Rostov-on-Don, Russia

A. S. Lyubukhin

Rostov State University of Economics (RINH), Rostov-on-Don, Russia

The article considers the problem of choosing the most effective control equipment for assessing the security parameters of an informatization object. As a solution, it is proposed to optimize the accuracy of the measuring instruments used in the equipment for given probabilities of false and undetected failure.

Keywords: control equipment, information security, optimal error, margin of error, recognition error, false and undetected failure.

Bibliography — 13 references.

Received June 25, 2023

Обеспечение информационной безопасности предприятия на основе риск-ориентированного подхода к проведению аудита информационной безопасности

В. В. Кабаков

Московский авиационный институт (национальный исследовательский университет),
Москва, Россия

Проведен анализ формирования основных требований по обеспечению информационной безопасности организации на основе проведения риск-ориентированного метода аудита информационной безопасности.

Ключевые слова: информация, аудит информационной безопасности, риск-ориентированный подход, защита информации.

Информационная безопасность (ИБ) представляет собой совокупность средств и методов, обеспечивающих возможность сохранения и защиты информации с ее ключевыми элементами. Примерами таких элементов являются системы и оборудование, используемое для работы с данной информацией. Таким образом, ИБ — это набор технологий, стандартов и методов управления, которые требуются для обеспечения защиты информации.

Цель обеспечения ИБ состоит в необходимости защиты информационных ресурсов и всей поддерживающей инфраструктуры от несанкционированного вмешательства. Именно такие вмешательства являются основной причиной потери данных или же их изменения. В результате использования средств ИБ обеспечивается непрерывность бизнеса [1].

Необходимо отметить, что успешная и эффективная интеграция систем ИБ на предприятиях может быть достигнута только при обеспечении трех основных принципов.

- **Конфиденциальность** — данное понятие включает в себя аспекты предотвращения нежелательного или же несанкционированного доступа к данным организации.

- **Целостность** — целостность обеспечивает внутреннюю и внешнюю последовательность предприятия. Помимо этого, именно данный принцип обеспечивает предотвращение искажения информации.

- **Доступность** — под данным понятием понимается надежный и эффективный доступ к информации. Компьютерные системы должны работать исправно и предсказуемо для возможности получения информации при такой необходимости.

Нарушение данных факторов может быть обусловлено в результате реализации угрозы информационной безопасности. Угроза ИБ представляет собой совокупность условий и факторов, которые создают опасность нарушения в работе системы информационной безопасности. Также под угрозой информационной безопасности понимается потенциально возможное событие или процесс, результат которого приводит к нарушению конфиденциальности, целостности или доступности информации [2].

Материалы и методы

При выполнении работы применяли такие методы научного исследования, как анализ и синтез. Помимо этого, использовали результаты научных исследований зарубежного и отечественного авторства. Именно на основе существующих результатов исследования методов проведения аудита информационной безопасности выполнены анализ и синтез информации для последующей систематизации материалов.

Результаты и обсуждение

Задачи по обеспечению информационной безопасности делятся на технические, административные, правовые и физические.

- **Технические.** К данным средствам защиты относят межсетевые экраны, антивирусные про-

Кабаков Виталий Валериевич, старший преподаватель.
E-mail: ser-kvv73@mail.ru

Статья поступила в редакцию 3 июля 2023 г.

© Кабаков В. В., 2023

граммы, системы шифрования, контроль и управление доступом и другое. В результате реализации данных мер каждому отдельному участнику рабочего процесса открывается персональный набор прав и функционал, согласно которым он может работать с информацией.

- *Административные.* К данной группе методов обеспечения ИБ относится, к примеру, запрет на использование сотрудниками организаций собственных цифровых устройств. Это простая мера и в то же время дающая высокие результаты эффективности обеспечения информационной безопасности для организации.

- *Правовые.* Правовые меры обеспечения ИБ включают наказание за преступления в области информационной безопасности. Помимо этого, к данной группе относится лицензирование деятельности и аттестация объектов информатизации.

- *Физические.* Физические системы защиты информации представляют один из самых больших сегментов обеспечения информационной безопасности. В ряд таких инструментов входят физические системы контроля и управления доступом, замки, сейфы, камеры наблюдения, лазерные сетки и множество других технических систем, препятствующих несанкционированному доступу к информации.

На сегодняшний момент времени происходит активное развитие, создание новых и улучшение существующих методов защиты информации. Вместе с разработкой аппаратно-программных инструментов активное развитие получают и различные методологические, организационные и правовые аспекты защиты информации. Одним из наиболее актуальных и показывающих эффективные результаты своего использования инструментом является аудит информационной безопасности организации.

Аудит информационной безопасности — это процесс оценки и проверки системы защиты информации в организации. Аудит проводят в целях выявления нарушений безопасности, оценки уровня риска и уязвимостей, а также определения необходимых мер для улучшения безопасности. Аудит может быть проведен как внутренними специалистами, так и сторонними экспертами. Результаты аудита используют для разработки плана мер по улучшению безопасности, обучения персонала, а также для улучшения процессов управления информационной безопасностью в организации [3].

Аудит информационной безопасности должен включать в себя проверку и оценку системы безопасности информации:

- оценку степени угрозы для информационной системы;

- проверку соответствия политикам и правилам безопасности информации;
- анализ доступа к информации и правильности настроек безопасности;
- проверку защиты от несанкционированного доступа;
- оценку устойчивости и надежности информационной системы при возникновении различных ситуаций;
- проверку соответствия законодательству и стандартам в области информационной безопасности.

Защита от угроз является основным компонентом снижения рисков ИБ. На рис. 1 представлен полный комплекс управления рисками информационной безопасности.

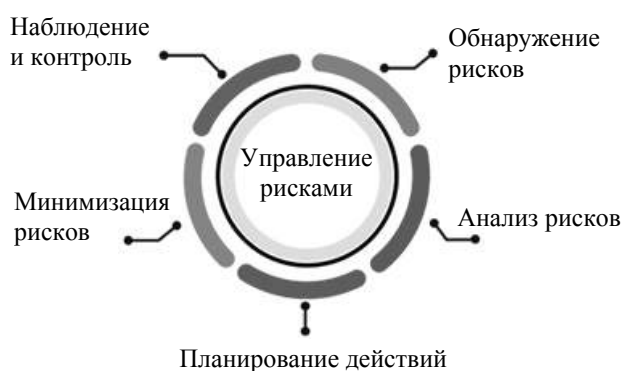


Рис. 1. Комплекс действий при управлении рисками ИБ

В результате аудита информационной безопасности могут быть выявлены недостатки и уязвимости системы безопасности, а также рекомендации по улучшению защиты информации. Так, результатом аудита информационной безопасности является отчет, где описывают: состояние системы информационной безопасности и ее риски; наличие и эффективность мер защиты от угроз; уровень управления безопасностью информации в организации; рекомендации по усовершенствованию системы информационной безопасности. Такой анализ поможет организациям определить слабые точки в защите информации и разработать планы по их устранению, повышению уровня информационной безопасности и уменьшению рисков [4].

Риск-ориентированный подход к аудиту ИБ — это метод, основанный на идентификации, оценке, контроле и управлении рисками, связанными с безопасностью информационных систем. Данный подход подразумевает наличие систематических процедур, инструментов и методов, которые помогают анализировать и оценивать риски в ИБ на стадии планирования, реализации и эксплуатации.

Риск-ориентированный подход позволяет выявлять уязвимости и определять наиболее значимые угрозы, которые могут нарушить безопасность информационной системы, а также определять эффективность контрольных мер, которые применяют для управления рисками безопасности информации. Основным принципом данного подхода является максимальная ориентация на защиту самых ценных активов организации и сокращение рисков до приемлемого уровня. Таким образом, риск-ориентированный подход к аудиту ИБ помогает улучшить уровень безопасности информационных систем организации и значительно снизить вероятность негативных последствий нарушения безопасности [5].

Риск-ориентированный подход к проведению аудита ИБ позволяет решить целый ряд задач, представленных на рис. 2.

Проведение аудита ИБ на основе риск-ориентированного подхода включает в себя пять основных действий, в составе каждого из которых можно выделить конкретное действие, значение и результат. Представленная ниже модель отражает каждый из этапов проведения данного аудита.

Этап 1. Проведение анализа бизнес-процессов:

1.1 Действие. Данный анализ помогает идентифицировать и документировать важные бизнес-процессы и лежащие в их основе зависимости, а также оценивать и ранжировать их на основе критичности. Технические и нетехнические факторы включены в качестве зависимостей (например, активы, персонал, данные, оборудование и приложения).

1.2 Значение. Анализ показывает, как эти ключевые операции и функции повлияют на непрерывность бизнеса, если они будут затруднены или устранены.

1.3 Результат. Проведение анализа влияния на бизнес — это первый шаг в создании планов обес-

печения непрерывности бизнеса и аварийного восстановления. Анализ идентифицирует критически важные бизнес-процессы и поддерживающие их элементы, помогая понять вашу среду и, что наиболее важно, прежде чем вы предпримете шаги для ее защиты.

Этап 2. Проведение оценки рисков:

2.1 Действие. Оценка риска — это количественный и качественный процесс, который выявляет угрозы, уязвимости и нормативные требования, применимые к соответствующим бизнес-процессам и базовым зависимостям. Затем он рассчитывает возможные последствия, если эти угрозы будут реализованы, то выдаст выходное значение риска.

Также важно отметить, что качественная и количественная оценки рисков ИБ могут работать в комплексе. При этом качественная оценка дает возможность именно получения представления о потенциальных проблемных областях, чтобы расставить их по степени важности. Результаты качественной и количественной оценки рисков могут быть использованы внутри компании или представлены аудитору по сертификации, проводящему дальнейшую работу с системой информационной безопасности [6].

2.2 Значение. Выходное значение риска дает руководству возможность понять и помочь определить приоритеты различных рисков, с которыми сталкивается организация. Этот результат является одним из самых больших преимуществ этого подхода, позволяющего создавать персонализированные показатели на основе вашей организации. По сравнению с использованием готовых обобщенных "рисков" для организации вашей программы кибербезопасности, которые могут не иметь значения и не защищать организацию от конкретных проблем, с которыми оно сталкивается.

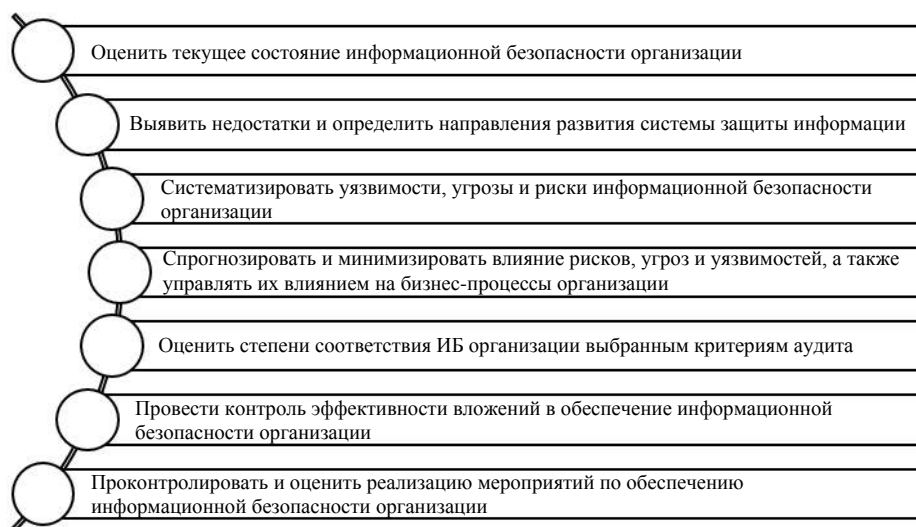


Рис. 2. Задачи риск-ориентированного подхода аудита ИБ

2.3 Результат. Знание выходного значения риска дает возможность ранжировать определенные уязвимости в реестре рисков; инструмент управления рисками, который объединяет результаты оценки рисков в одном месте. Реестр рисков обеспечивает действенную отправную точку для сосредоточения стратегических ресурсов на снижении рисков, представляющих наибольшую угрозу для непрерывности бизнеса и соблюдения нормативных требований.

Этап 3. Определение и внедрение необходимых средств контроля:

3.1 Действие. на этом этапе эксперт берет во внимание наиболее опасные риски, определяет, адаптирует, внедряет и назначает ответственность за элементы управления, которые смогут их уменьшить. Средство контроля — это основанное на действиях заявление, в котором содержатся инструкции о том, как уменьшить или свести к минимуму риски безопасности. Примеры систем контроля кибербезопасности: NIST 800-53, CIS, HITRUST CSF, ISO 27001/27002, COBIT, PCI DSS. Это предварительно упакованные средства управления безопасностью в отрасли рисков, которые можно настроить для каждой конкретной организации.

3.2 Значение. Персонализированные риски позволяют организации лучше настраивать средства контроля для устранения выявленных уязвимостей и угроз. Это также позволяет организации использовать компенсирующие меры, поскольку весь процесс принятия решений документируется. Документация демонстрирует, что организация понимает угрозу, которую средство контроля должно покрывать, и адекватно применяет другие компенсирующие средства контроля на основе анализа затрат и рисков [7].

3.3 Результат. Определение и внедрение правильных или необходимых средств контроля обеспечивает структуру и возможность обновлять или создавать политики и процедуры, которые укрепляют и передают видение и приоритеты организации в отношении ее кибербезопасности. Точно так же этот подход может обеспечить более активное участие и соблюдение требований, поскольку он создает возможность для диалога с отдельными заинтересованными сторонами, которые "владеют" процессом, включая поддержку со стороны критически важного руководства среднего звена. По сути, этот подход, основанный на оценке рисков, дает руководству убедительную причину для адаптации и принятия решений при бездействии и возможных последствий.

Этап 4. Тестирование, проверка и отчет:

4.1 Действие. После того, как средства безопасности будут реализованы, их необходимо

протестировать и подтвердить. Примеры различных типов тестирования включают тесты на проникновение, дополнительные оценки рисков, тесты управления уязвимостями, упражнения на обеспечение непрерывности бизнеса, внутренние аудиты и оценки контроля соответствия.

4.2 Значение. Тестирование и проверка дают не только уверенность в том, что элементы управления работают и обеспечивают необходимую безопасность, но и при периодической переоценке предоставляют возможность включения недавно реализованных элементов управления безопасностью. Теперь руководство может получить новую оценку стоимости риска, называемую остаточным риском, которую документируют и добавляют в реестр рисков для будущего анализа и определения приоритетов. Основываясь на инвестициях в новый контроль, рейтинг риска может снизиться, что указывает на совершенствование системы ИБ.

4.3 Результат. Действия по тестированию и проверке должны быть задокументированы и зарегистрированы. Наличие эффективного механизма отчетности демонстрирует прогресс на пути к исполнительному руководству и соответствие требованиям регулирующих органов. Кроме того, эффективная отчетность закладывает основу для создания процессов устранения рисков.

Этап 5. Непрерывный мониторинг и управление:

5.1 Действие. На этом последнем этапе цель — оформить этапы 1—4 в воспроизводимый бизнес-процесс. Оценки рисков необходимо проводить не реже одного раза в год, а действия по устранению последствий должны быть осуществлены, проконтролированы и включены в реестр рисков. Кроме того, должны быть созданы механизмы отчетности для внутренних сотрудников, чтобы выявлять и сообщать о потенциальных рисках для организации. Часто у менеджеров и других сотрудников есть важные сведения о слабых сторонах или нарушениях нормативно-правовых требований, которые могут быть скрыты от группы управления рисками. Если организация придерживается всего цикла, то точно обнаружит пробелы в процессах либо из-за плохо реализованных средств контроля, либо из-за упущений в процессе выявления рисков [8].

5.2 Значение. Соблюдение цикла может гарантировать, что любые новые уязвимости или угрозы будут выявлены и устранены последовательно и своевременно, что снизит вероятность того, что основные проблемы останутся незамеченными. На этом этапе сотрудники могут отмечать проблемы, уведомлять организацию, а также оценивать ущерб в случае эксплуатации.

5.3 Результат. Непрерывное управление на протяжении всего жизненного цикла подхода, основанного на оценке рисков, будет способствовать подотчетности за внедрение и оценку средств контроля. Это создает пути эскалации для сложных или несоответствующих заинтересованных сторон и обеспечивает последовательность в адаптации контроля. Наконец, цикл предоставляет возможность обновлять или создавать необходимые политики или процедурную документацию и последовательно сообщать об изменениях в организацию.

Также важным шагом может быть внедрение комплексной методологии количественного анализа рисков, которая использует менее предвзятую и более измеримую информацию для изучения уязвимостей, вызывающих наибольшее беспокойство. Затем эти результаты могут быть использованы внутри компании или предоставлены аудиту по сертификации, проводящему дальнейшую оценку соответствия.

Заключение

Выполнен анализ по вопросу обеспечения защиты информации в организации на основе проведения риск-ориентированного метода аудита информационной безопасности. В результате работы определены основные особенности, преимущества и актуальность использования данного метода. В работе подтверждена гипотеза о возможности повышения качества и эффективности функционирования предприятия в результате использования риск-ориентированного аудита информационной безопасности по определенным требованиям.

В заключение необходимо отметить, что во многих компаниях активно практикуется риск-ориентированный подход, когда решения о реализации мер защиты и совершенствовании системы ИБ принимаются на основе оценки рисков, согласно принятым в индустрии методологиям и практикам. Качественно выстроенный процесс

риск-менеджмента позволит руководителю ИБ самостоятельно определять необходимый набор мер для снижения рисков и поможет сэкономить бюджет, а также обосновать выделение дополнительных ресурсов на защиту новых сфер деятельности компании.

Так, аудит ИБ на основе риск-ориентированного подхода может предоставить руководителям организаций возможность получить независимый взгляд на существующую систему ИБ и выявить шаги, необходимые для совершенствования системы информационной безопасности. Данный аудит дает оценку защищенности компании, выявляет риски и создает план конкретных действий, направленных на минимизацию их влияния.

Литература

1. Попов В. Г., Галиаскаров Д. Ф., Гвоздев Л. Б. Актуальность обеспечения информационной безопасности в сетях IoT // Научно-образовательный журнал для студентов и преподавателей "StudNet". 2021. № 4. — 6 с.
2. Тимербулатов Т. А., Юсупов Р. Г. Информационная безопасность: об актуальности исторического исследования проблемы // Инновационная наука. 2019. № 9. С. 23—27.
3. Сапожников И. В., Муранова М. А., Тюкова А. Д., Суханов Е. Э. О методике аудита информационной безопасности информационной системы персональных данных некоммерческой организации // The Scientific Heritage. 2021. № 63-1 (63). С. 50—53.
4. Макаренко С. И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. № 1. С. 1—29.
5. Двойнишников Н. Э., Исламутдинова Д. Ф. Понятие и сущность аудита безопасности информационных систем // Московский экономический журнал. 2019. № 10. С. 67.
6. Картак В. М., Гатиятуллин Т. Р. Методология анализа рисков информационной безопасности в банковском секторе с использованием нечеткой логики // Проблемы науки. 2018. № 2(26). С. 8—9.
7. Агринский Н. М. Количественный анализ рисков информационной безопасности с необходимой точностью в соответствии с требованиями международного стандарта ISO 27001:2013 // Инновации и инвестиции. 2020. № 6. С. 88—92.
8. Баранова Е. К. Методики анализа и оценки рисков информационной безопасности // Образовательные ресурсы и технологии. 2015. № 1(9). С. 73—79.

Ensuring the information security of an enterprise based on a risk-based approach to conducting an information security audit

V. V. Kabakov

Moscow Aviation Institute (National Research University), Moscow, Russia

The purpose of the current article is to analyze the issue and form the basic requirements for ensuring the information security of an organization based on the risk-based method of information security audit.

Keywords: information, information security audit, risk-based approach, information protection.

Bibliography — 8 references.

Received July 3, 2023

Киберустойчивость предприятий пищевой промышленности: определение потенциальных векторов атаки

С. Ю. Сидорин; И. Г. Благовещенский, д-р техн. наук; Е. А. Соболева
ФГБОУ ВО «Российский биотехнологический университет (РОСБИОТЕХ)», Москва, Россия

В. И. Шармаев

Московский авиационный институт (национальный исследовательский университет),
Москва, Россия

Проведено исследование, цель которого выявление критических сетевых сервисов предприятия пищевой промышленности и оценка возможных последствий успешных атак на эти сервисы. Исследование проводили с использованием смоделированной среды и инструментов сетевого сканирования для оценки общей киберустойчивости сети. В качестве исследовательской среды был выбран эмулятор сети Mininet, а для идентификации устройств в сети и поиска открытых портов использовали инструмент сетевого сканирования Nmap. Топология сети, состоящая из 22 хостов и 4 коммутаторов, представляет собой различные отделы мукомольного предприятия: отдел производства, отдел логистики, отдел продаж и отдел кадров. Главным выводом эксперимента является тот факт, что злоумышленник может идентифицировать все устройства в сети и выполнить полное сканирование всех открытых портов на каждом устройстве, потенциально выявив слабые места в сети. Исследуя конкретные отделы в инфраструктуре мукомольного предприятия, авторы определяли возможные сетевые сервисы, которые можно использовать для выполнения соответствующих им бизнес-функций, и проанализировали потенциальные последствия эксплуатации уязвимостей и кибератаки на каждый из них. Исследование дает представление о потенциальных векторах атак на предприятия пищевой промышленности, выделяя области, требующие внимания для повышения киберустойчивости сети.

Ключевые слова: киберустойчивость, информационная безопасность, сетевая разведка, Mininet, Nmap.

Распространение сетевых устройств и систем в пищевой промышленности принесло отрасли значительные преимущества, начиная от повышения производительности и заканчивая улучшением безопасности и контроля качества продуктов питания [1, 2]. Однако эти достижения также подвергли отрасль новым киберугрозам, что подчеркивает необходимость разработки надежных стратегий защиты для обеспечения бесперебойной работы предприятий [3].

Пищевая промышленность имеет некоторые уникальные характеристики, отличающие ее от

других предприятий. Любой сбой или компрометация процессов производства продуктов питания могут иметь серьезные последствия для здоровья и безопасности населения [4]. В отличие от некоторых других отраслей, последствия инцидента кибербезопасности в отрасли пищевой промышленности могут выйти за рамки финансовых потерь и репутационного ущерба и непосредственно повлиять на благосостояние людей [5].

Пищевая промышленность часто опирается на сложные и глобальные цепочки поставок, включающие множество поставщиков, дистрибьюторов и розничных торговцев. Такая сложность увеличивает потенциальную поверхность атаки и повышает сложность поддержания кибербезопасности во всей цепочке поставок [6].

Кроме того, в пищевой промышленности используют специализированные системы и технологии, предназначенные для производства продуктов питания, такие, как системы автоматизации процессов и системы диспетчерского контроля и сбора данных (SCADA) [7, 8]. Эти системы могут иметь уникальные уязвимости, которые, в свою очередь, требуют особого подхода [9]. Кроме того, интеграция новых технологий, таких, как устрой-

Сидорин Сергей Юрьевич, аспирант.

E-mail: sarmatsid@yandex.ru

Благовещенский Иван Германович, профессор кафедры "Информатика и вычислительная техника пищевых производств".

E-mail: blagvig@yandex.ru

Соболева Елизавета Александровна, студент.

E-mail: soboleva_ss@gmail.com

Шармаев Вадим Игоревич, аспирант.

E-mail: vadiidq@yandex.ru

Статья поступила в редакцию 31 мая 2023 г.

© Сидорин С. Ю., Благовещенский И. Г., Соболева Е. А., Шармаев В. И., 2023

ства Интернета вещей (IoT) и интеллектуальные датчики на пищевых предприятиях, создает новые векторы атак, которые также необходимо учитывать при проектировании систем защиты [10, 11].

Мукомольные предприятия являются важнейшей частью цепи поставок продовольствия, производя один из самых важных основных продуктов питания в мире, поэтому они, несомненно, являются привлекательной целью для злоумышленников [12]. Чтобы всесторонне оценить возможные риски и уязвимости пищевого производства, учитывая описанные отличительные особенности, необходимо понимать, из каких компонентов складывается инфраструктура сети предприятия.

Для данного исследования авторы выбрали следующие отделы в качестве ключевых компонентов [13].

- *Производственный отдел* — включает в себя оборудование и системы, отвечающие за переработку зерна, помол и производство муки.
- *Отдел логистики* — управляет закупкой, хранением и распределением сырья и готовой продукции на мукомольном предприятии.
- *Отдел продаж* — контролирует маркетинг, продажи и распространение продукции мукомольного предприятия.
- *Отдел кадров* — обеспечивает выполнение таких процессов управления персоналом, как учет сотрудников, начисление заработной платы и выплату пособий.

Материалы и методы

Цель данного исследования — определить критически важные сетевые сервисы предприятия пищевой промышленности (на примере мукомольного предприятия) и оценить потенциальные последствия атаки на эти сервисы. Объектом исследования является сеть предприятия, которая

проанализирована с помощью моделируемой среды и инструментов сетевого сканирования для выявления потенциальных уязвимостей и оценки общей киберустойчивости сети.

Исследовательская среда. Исследование проводилось с использованием эмулятора сети *Mininet*, который создает виртуальную сетевую среду и позволяет моделировать различные сетевые протоколы и службы. Инструмент предоставляет *Python API* для создания и управления топологией сети и сетевым трафиком [14, 15]. Запуск виртуальной сетевой среды происходил на компьютере с процессором *Intel Core i5* с 8 ГБ оперативной памяти и операционной системой *Ubuntu 22.04.01*.

Программные инструменты. В ходе эксперимента выполнялся программный код, написанный с использованием языка программирования *Python 3.10.6*. В выполняемом программном коде была подключена библиотека *Mininet 2.3.0* (для создания топологии виртуальной сети). Также для идентификации устройств в сети и поиска открытых портов был использован инструмент сетевого сканирования *Nmap*, предназначенный для сканирования сетей, идентификации узлов и служб, а также обнаружения уязвимостей [16, 17].

Используемые устройства. В эксперименте использована топология сети *Mininet* с 22 хостами и 4 коммутаторами. Топология включала 4 сегмента сети, каждый из которых соответствовал отделу мукомольного предприятия: отделу производства, отделу логистики, отделу продаж и отделу кадров. Каждый сегмент состоял из коммутатора и нескольких рабочих станций (хостов) с адресами в частной подсети 10.0.0.0/24. Технические характеристики хостов: процессор *Intel Core i5*, оперативная память 8 ГБ, операционная система *Ubuntu 22.04.01*. Хосты оснащены сетевой интерфейсной картой 100 Мбит/с. Топология сети представлена на рис. 1.

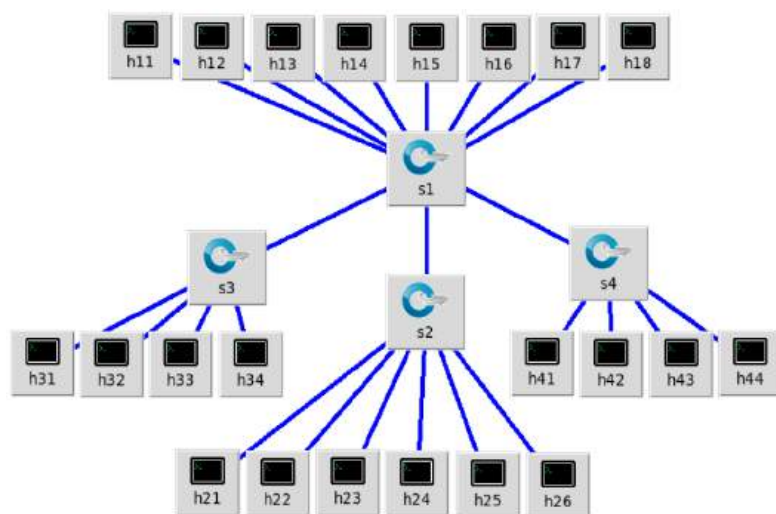


Рис. 1. Топология сети

В ходе эксперимента были сделаны следующие допущения и сформулированы соответствующие им обоснования.

- Используемая топология точно представляет инфраструктуру сети мукомольного предприятия. Предполагается, что на предприятии пищевой промышленности есть различные отделы, такие, как отдел производства, отдел логистики, отдел продаж и отдел кадров.

- Конкретные сетевые службы, используемые в каждом отделе предприятия, точно представлены открытыми портами на устройствах в этих отделах. Открывая эти порты, авторы имитируют реальную сетевую среду мукомольного предприятия.

- Выполненное сканирование точно отражает текущее состояние сети и устройств в ней (команды Nmap, используемые в эксперименте, широко используют специалисты по безопасности для сбора информации о сети [18]).

Кроме того, эксперимент направлен, в первую очередь, на идентификацию устройств и открытых портов и не включает расширенное тестирование на проникновение или оценку конкретных уязвимостей в сетевых службах или приложениях.

Общий алгоритм эксперимента. Инициализация топологии сети *Topo*. Создание симуляции *Mininet* с топологией *Topo* и *TCLink* для конфигурации соединений. Запуск симуляции *Mininet*. Открытие на устройствах портов, характерных для сетевых служб, используемых в различных отделах предприятия. Запуск терминала на хосте *h11* с помощью команды *xterm*. Выполнение сканирования всей сети с помощью команды *nmap -sn* для

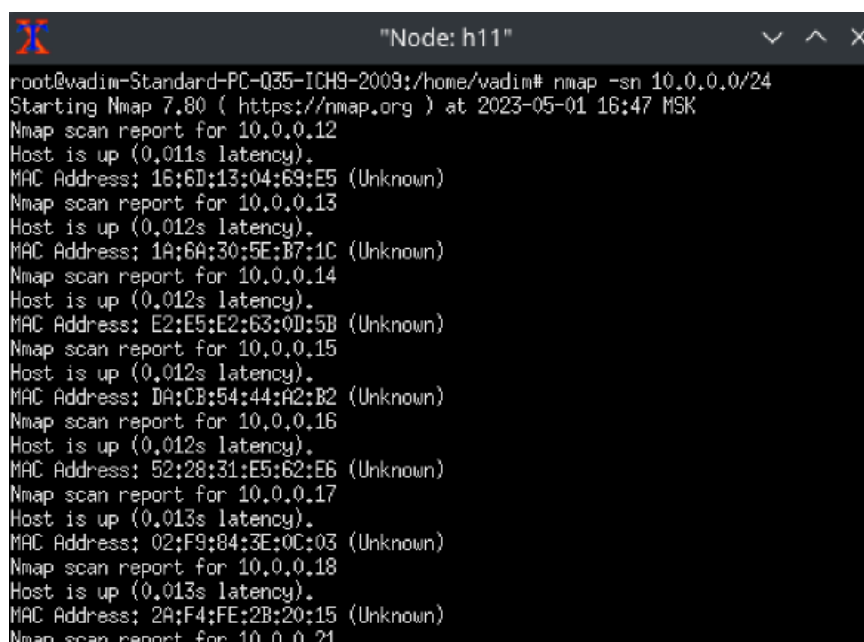
идентификации всех устройств в сети. Выполнение команды *nmap -p-* для каждого устройства в сети для обнаружения всех открытых портов устройств. Остановка симуляции *Mininet*.

Команда *nmap -sn*, используемая для идентификации устройств в сети, посылает эхо-запрос ICMP каждому узлу в сети и ждет ответа. Ответы используют для определения IP-адресов узлов в сети [19]. Команда *nmap -p-* сканирует все 65535 портов на указанном хосте и сообщает, какие порты открыты и какие службы прослушивают эти порты [20].

Ожидаемые результаты эксперимента включают идентификацию устройств в сети мукомольного предприятия и обнаружение открытых портов, связанных с конкретными сетевыми службами. Собранные данные обработаны и проанализированы для оценки киберустойчивости сети мукомольного предприятия. Результаты дали представление о потенциальных векторах атаки, тем самым выделив области, требующие внимания для повышения киберустойчивости сети.

Результаты

После открытия портов на устройствах, специфичных для сетевых служб, используемых в различных отделах предприятия, было проведено сканирование всей сети с помощью команды *nmap -sn*. В ходе сканирования были определены все устройства в сети и соответствующие им IP-адреса. Отображение в консоли хоста *h11* выполняемой команды и ее результатов представлены на рис. 2.



```
root@vadin-Standard-PC-Q35-ICH9-2009:/home/vadin# nmap -sn 10.0.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-05-01 16:47 MSK
Nmap scan report for 10.0.0.12
Host is up (0.011s latency).
MAC Address: 16:6D:13:04:69:E5 (Unknown)
Nmap scan report for 10.0.0.13
Host is up (0.012s latency).
MAC Address: 1A:6A:30:5E:B7:1C (Unknown)
Nmap scan report for 10.0.0.14
Host is up (0.012s latency).
MAC Address: E2:E5:E2:63:0D:5B (Unknown)
Nmap scan report for 10.0.0.15
Host is up (0.012s latency).
MAC Address: DA:CB:54:44:A2:B2 (Unknown)
Nmap scan report for 10.0.0.16
Host is up (0.012s latency).
MAC Address: 52:28:31:E5:62:E6 (Unknown)
Nmap scan report for 10.0.0.17
Host is up (0.013s latency).
MAC Address: 02:F9:84:3E:0C:03 (Unknown)
Nmap scan report for 10.0.0.18
Host is up (0.013s latency).
MAC Address: 2A:F4:FE:2B:20:15 (Unknown)
Nmap scan report for 10.0.0.21
```

Рис. 2. Выполнение команды *nmap -sn*

Для каждого устройства было выполнено сканирование всех открытых портов с помощью команды *ntar -p-*. Результаты сканирования представлены в таблице.

Обнаруженные открытые порты

Ключевые компоненты	Устройство	Порт	Сетевая служба
Отдел производства	h12	502	Modbus
	h13	3306	MySQL
	h14	4480	ROCLINK
	h15	44818	EtherNet/IP
Отдел логистики	h21	21	FTP
	h22	80	HTTP
	h23	445	SMB
	h24	3306	MySQL
Отдел продаж	h31	110	POP3
	h32	587	SMTP
	h33	3306	MySQL
Отдел кадров	h41	443	HTTPS
	h42	3306	MySQL
	h43	3389	RDP

Отображение в консоли хоста *h11* выполняемой команды и ее результатов для двух первых обнаруженных устройств в сети представлены на рис. 3.

Из результатов сканирования видно, что в сети предприятия работают различные сетевые службы. Эта информация потенциально может предоставить злоумышленникам возможность использовать уязвимости и нарушить киберустойчивость сети. Незащищенные службы могут быть использованы как для получения несанкционированного доступа к конфиденциальным данным, так и для совершения атак на сеть предприятия.

Обсуждение

Обсудим возможное применение каждой сетевой службы и последствия эксплуатации их уязвимостей.

В производственном отделе были идентифицированы следующие сетевые службы и открыты для сканирования соответствующие им порты:

Modbus (порт 502) — протокол связи, обычно используемый системами диспетчерского управления и сбора данных (*SCADA*-системами). Сетевая служба позволяет системе *SCADA* собирать данные и отправлять команды на устройства, обеспечивая автоматизацию и мониторинг производственного процесса [21]. Атака на сетевую службу может нарушить производственные процессы на предприятии, что приведет к задержкам производства, простоем оборудования, ошибкам в производстве или даже физическому повреждению оборудования.

```

"Node: h11"
root@vadim-Standard-PC-Q35-ICH9-2009:/home/vadim# nmap -p- 10.0.0.12
Starting Nmap 7.80 ( https://nmap.org ) at 2023-05-01 16:55 MSK
Nmap scan report for 10.0.0.12
Host is up (0.049s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE
502/tcp   open  modbus
MAC Address: 16:60:13:04:69:E5 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 46.83 seconds
root@vadim-Standard-PC-Q35-ICH9-2009:/home/vadim# nmap -p- 10.0.0.13
Starting Nmap 7.80 ( https://nmap.org ) at 2023-05-01 16:56 MSK
Nmap scan report for 10.0.0.13
Host is up (0.045s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE
44818/tcp open  EtherNetIP-2
MAC Address: 1A:6A:30:5E:B7:1C (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 65.70 seconds
root@vadim-Standard-PC-Q35-ICH9-2009:/home/vadim#

```

Рис. 3. Выполнение команды *ntar -p-* для хостов *h12* и *h13*

MySQL (порт 3306) — это популярная система управления реляционными базами данных с открытым исходным кодом [22]. В отделе производства *MySQL* может быть использована для хранения и управления различными данными, связанными с производством, такими, как производственные запасы, параметры производственных процессов, данные контроля качества [23]. Атака на сетевую службу может привести к несанкционированному доступу, манипулированию данными или даже их потере, что поставит под угрозу целостность, конфиденциальность и доступность информации, связанной с производственными процессами, а также может привести к неточному учету запасов или снижению качества продукции.

ROCLINK (порт 4480) — это проприетарный протокол, используемый для настройки и мониторинга контроллеров удаленного управления (устройств *ROC*), которые широко применяют в системах автоматизации и управления технологическими процессами [24]. Протокол также может быть использован в процессе помола муки для контроля и управления машинами и оборудованием предприятия. Атака на сетевую службу может потенциально нарушить процессы управления производством или предоставить злоумышленнику возможность манипулировать ими, что приведет к неисправности оборудования и остановке производственных процессов.

EtherNet/IP (порт 44818) — это промышленный протокол *Ethernet*, используемый для связи в реальном времени между устройствами в системах промышленной автоматизации и обеспечивающий обмен данными между различными компонентами производственной системы (между оборудованием различных производителей) [25]. Его также можно использовать в процессе помола муки для контроля и управления машинами и оборудованием. Атака на сетевую службу может привести к перехвату данных между различными компонентами производства, либо предоставит злоумышленнику возможность манипулировать ими и нарушить производственный процесс.

В отделе логистики были идентифицированы следующие сетевые службы и открыты для сканирования соответствующие им порты:

FTP (порт 21) — это протокол передачи файлов по сети [26], который может быть использован в отделе логистики для обмена документами, связанными с доставкой или транспортировкой, такими как счета-фактуры, декларации или заказы на поставку. Атака на сетевую службу может привести к несанкционированному доступу и краже конфиденциальных документов, связанных с ло-

гистикой (например, транспортные накладные, графики доставки), а также может предоставить злоумышленнику возможность манипулировать ими, что может привести к сбоям в цепи поставок, ошибкам в доставке и финансовым потерям.

HTTP (порт 80) — это протокол прикладного уровня передачи данных в виде гипертекстовых документов в формате *HTML* (в настоящее время — для передачи произвольных данных) [27, 28]. В отделе логистики мукомольного предприятия *HTTP* может быть использован для доступа к веб-системам управления логистикой, отслеживания состояния груза или получения информации от поставщиков логистических услуг. Атака на сетевую службу может обеспечить злоумышленнику несанкционированный доступ к важным логистическим данным, что может поставить под угрозу конфиденциальность, целостность и доступность логистических операций.

SMB (порт 445) — это сетевой протокол, используемый для совместного использования файлов, печати и связи между узлами сети [29]. В отделе логистики *SMB* может быть использован для совместного доступа к файлам или ресурсам, связанным с логистикой (например, для совместного доступа к данным об отгрузке и доставке). Атака на сетевую службу может привести к несанкционированному доступу, утечке данных или распространению вредоносного ПО в логистической сети.

MySQL (порт 3306) в отделе логистики может быть использован для хранения записей о доставке, информации о клиентах или данных логистической аналитики. Атака на службу *MySQL* может нарушить конфиденциальность, целостность и доступность логистических данных, и, как следствие, привести к сбоям в логистических операциях.

В отделе продаж были идентифицированы следующие сетевые службы и открыты для сканирования соответствующие им порты:

POP3 (порт 110) — это протокол получения электронной почты [30]. В отделе продаж протокол может использоваться для получения электронной почты, связанной с продажами. Атака на службу *POP3* потенциально может привести к несанкционированному доступу к электронной почте, раскрытию конфиденциальной информации о клиентах, стратегиях продаж или финансовых данных.

SMTP (порт 587) — это протокол доставки электронной почты [31]. В отделе продаж *SMTP* может быть использован для отправки исходящих электронных сообщений, связанных с продажами, например, подтверждений заказов или маркетинговых сообщений. Атака на сетевую службу мо-

жет привести к несанкционированному доступу, перехвату или модификации электронной почты отдела продаж, что может повлиять на связь с клиентами, отношения с поставщиками или репутацию предприятия.

MySQL (порт 3306) в отделе продаж может быть использована для хранения информации о клиентах, данных о продажах или записей системы управления взаимоотношениями с клиентами (CRM) [32]. Атака на сетевую службу может привести к несанкционированному доступу, манипулированию данными или утечке данных, что, в свою очередь, может привести к финансовым и репутационным потерям.

В отделе кадров были идентифицированы следующие сетевые службы и открыты для сканирования соответствующие им порты:

HTTPS (порт 443) — это зашифрованная версия протокола *HTTP*, которая обеспечивает безопасную передачу данных по сети [33]. В отделе кадров *HTTPS* может быть использован для доступа работников к веб-порталу, содержащему информацию о заработной плате. Атака на сетевую службу *HTTPS* потенциально может привести к краже этой конфиденциальной информации.

MySQL (порт 3306) в отделе кадров может быть использована для хранения данных сотрудников, кадровых документов или информации о заработной плате. Атака на службу *MySQL* может привести к несанкционированному доступу к конфиденциальной информации, краже личных данных или мошенническим действиям в отношении сотрудников.

RDP (порт 3389) — это протокол удаленного рабочего стола, который обеспечивает доступ к компьютерам или серверам через сетевое соединение [34]. В отделе кадров *RDP* может использоваться для удаленного администрирования или удаленного доступа к системам и приложениям отдела. Атака на службу *RDP* может привести к несанкционированному доступу к ресурсам *HR* и конфиденциальным данным сотрудников, к утечке данных, несанкционированным изменениям или компрометации критически важных функций, таких, как обработка платежных ведомостей, управление сотрудниками или деятельности, связанной с соблюдением нормативных требований.

Таким образом, разведка сети может выявить потенциальные риски, связанные с открытыми сетевыми сервисами в сети мукомольного предприятия. Последствия успешных атак на эти сервисы могут включать в себя серьезные сбои в процессах производства, логистики, продаж и работы с персоналом. Для предприятий пищевой промышленности крайне важно уделять приоритетное

внимание кибербезопасности и активно устранять уязвимости, чтобы защитить свою деятельность, данные клиентов и репутацию предприятия.

Заключение

С помощью моделирования сетевой инфраструктуры предприятия пищевой промышленности и комплексного сканирования авторами были определены критически важные сетевые сервисы, специфичные для различных отделов, и оценены потенциальные последствия успешных атак на эти сервисы.

Разведывательное сканирование выявило несколько векторов атак в сети мукомольного предприятия. Открытые порты и сервисы обеспечивают потенциальные точки входа для злоумышленников. Нарушение работы сетевых служб может привести к значительным сбоям в производственных процессах, к простоям, снижению производительности и потенциальному повреждению оборудования. Атаки на сетевые службы, используемые в отделе логистики, могут привести к задержкам поставок, неточностям в инвентаризации и сбоям в управлении цепочкой поставок. Любое нарушение или компрометация служб в отделе продаж может иметь серьезные последствия, включая несанкционированный доступ к конфиденциальной информации о клиентах, перехват электронной почты и потенциальную утечку данных. Наконец, атака на сетевые сервисы отдела кадров может привести к раскрытию конфиденциальных данных сотрудников, информации о заработной плате и личных данных.

Результаты данного исследования демонстрируют важность внедрения надежных мер обеспечения кибербезопасности для защиты от потенциальных атак. Такие меры могут включать регулярную оценку уязвимостей, тестирование на проникновение, сегментацию сети и обучение сотрудников. Кроме того, для предприятий пищевой промышленности крайне важно иметь план реагирования на инциденты, чтобы быстро реагировать на любые кибератаки и минимизировать их влияние на бизнес [35].

Стоит, однако, учитывать, что эксперимент не учитывал применение каких-либо защитных мер, таких, как брандмауэры или системы обнаружения вторжений. Дальнейшие направления исследования могут включать проведение более полного анализа потенциальных угроз и уязвимостей, с которыми сталкиваются мукомольные предприятия и другие предприятия пищевой промышленности. Для этого потребуется использование более совершенных инструментов сканирования, тести-

рования на проникновение и методов социальной инженерии для выявления слабых мест в системе и определения уровня риска.

Литература

1. Коротков Д. В., Ермишин А. С. Трансформация предприятия пищевой промышленности в контексте цифровизации // Цифровая трансформация промышленности: тенденции, управление, стратегии. 2019. С. 312—320.
2. Голицыцкий П. В. и др. Влияние цифровизации на эффективность технологических процессов современного производства // Компетентность. 2021. № 8. С. 48—54.
3. Деркачева Е. А. и др. Основы цифровой экономики. — Краснодар: Новация, 2021. С. 20—21.
4. Шилов В. В. и др. Пищевая промышленность: наука и технологии // Пищевая промышленность. 2022. Т. 15. № 3. С. 90—98.
5. Michael K. et al. Privacy, data rights and cybersecurity: Technology for good in the achievement of sustainable development goals // 2019 IEEE International Symposium on Technology and Society (ISTAS). IEEE, 2019. P. 1—13.
6. Миронова О. В., Делятицкая А. В. Цифровая трансформация социально-экономических систем в Российской Федерации // Управленческий учет. 2021. № 9-1. С. 133—139.
7. Художерко Е. Е. Применение SCADA-систем в пищевой промышленности // Ответственный редактор. 2021. С. 99.
8. Аметов Ф. Р., Бекиров Э. А. Причинный анализ критических уязвимостей системы контроля и сбора данных SCADA // Строительство и техногенная безопасность. 2019. № 15(67). С. 135—140.
9. Белозеров В. В., Кречетов А. Л., Олейников С. Н. Об информационной безопасности автоматизированных систем управления // Электроника и электротехника. 2018. № 4. С. 24—39.
10. Nychas G. J. et al. Data science in the food industry // Annual Review of Biomedical Data Science. 2021. V. 4. P. 341—367.
11. Misra N. N. et al. IoT, big data, and artificial intelligence in agriculture and food industry // IEEE Internet of things Journal. 2020. V. 9. № 9. P. 6305—6324.
12. Лисицына Ю. А. Анализ факторов устойчивого роста предприятий мукомольной отрасли // Вестник ИЭАУ. 2020. № 29. С. 7.
13. Авто В. Г. и др. Разработка системы комплексной автоматизации предприятия пищевой промышленности // Хранение и переработка сельхозсырья. 2018. № 2. С. 92—99.
14. Наливайко С. М. Автоматизация процессов моделирования и измерения сетевых характеристик в Mininet // Информационно-телекоммуникационные технологии и математическое моделирование высокотехнологичных систем. 2022. С. 397—403.
15. Дмитриева Ю. С. Сравнительный анализ методов управления сетевыми ресурсами в сетях SDN // Труды учебных заведений связи. 2022. Т. 8. № 1. С. 73—83.
16. Куличенко В. Д. и др. Активное и пассивное сканирование портов как этап проведения сетевой атаки: Межд. науч.-практич. конф. "XCVI Международные научные чтения (памяти Г. Н. Бабакина)". 2020. С. 5—7.
17. Coffey K. et al. Vulnerability analysis of network scanning on SCADA systems // Security and Communication Networks. 2018. V. 2018.
18. Журавлев Е. Н. Методы обнаружения сетевых устройств // Молодежь и наука 2023: к вершинам познания. 2023. С. 154—159.
19. Shah M. et al. Penetration testing active reconnaissance phase—optimized port scanning with nmap tool // 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET). IEEE, 2019. P. 1—6.
20. Куреев А. П., Онищук С. Ю., Гулин Д. С. Сбор и анализ сетевого трафика посредством сканирования сети различными методами // Достижения вузовской науки 2018. 2018. С. 114—117.
21. Kalech M. Cyber-attack detection in SCADA systems using temporal pattern recognition techniques // Computers & Security. 2019. V. 84. P. 225—238.
22. Марченко В. Ю. СУБД MySQL // Молодежь и актуальные проблемы современной науки — 2018.
23. Рябов А. И., Штерензон В. А. Автоматизированная система учета готовой маркированной продукции // Инновации. Наука. Образование. 2021. № 38. С. 605—617.
24. Popa S. The Read-Out Controller (ROC) // The Read-Out Controller ASIC for the ATLAS Experiment at LHC. — Cham: Springer International Publishing, 2022. P. 33—78.
25. Смоляк С. Д., Петров С. Н., Пулко Т. А. Мониторинг техногенных объектов, доступных из сети Интернет // Доклады Белорусского государственного университета информатики и радиоэлектроники. 2019. № 6(124). С. 80—86.
26. Кистерев В. Р., Газизов А. Р. Технические аспекты защиты протоколов передачи файлов // Инновационное развитие. 2018. № 10. С. 19—20.
27. Ghedini A., Lalkaka R. HTTP/3: The past, the present, and the future // The Cloudflare Blog. 2019. P. 1.
28. Садовский В. Т., Скрылев Н. П. Основы сетевых технологий. — Могилев: Белорус.-Рос ун-т. 2022. С. 111—112.
29. Муратов Г. А. Анализ протокола SMB и его безопасность // Научно-практические исследования. 2021. № 4-2. С. 8—10.
30. Нemiшлова А. Г., Федотов Е. А. Использование почтового протокола POP3 для получения сообщений электронной почты с почтового сервера: XII Международный молодежный форум "Образование. Наука. Производство". 2020. С. 1934—1939.
31. Karamollahi M., Williamson C. Characterization of IMAPS email traffic // 2019 IEEE 27th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS). IEEE, 2019. P. 214—220.
32. Климочкина Л. А., Чабаненко А. В. Внедрение CRM системы в организации // Метрологическое обеспечение инновационных технологий. 2021. С. 20—21.
33. Шинкарев Н. Н., Толкачева Е. В. Автоматизация анализа сетевого трафика в целях предотвращения инцидентов информационной безопасности // Архитектурно-строительный и дорожно-транспортный комплексы: проблемы, перспективы, инновации. 2022. С. 614—620.
34. Badhwar R. Security Controls for Remote Access Technologies // The CISO's Next Frontier: AI, Post-Quantum Cryptography and Advanced Security Paradigms. — Cham: Springer International Publishing, 2021. С. 99—104.
35. Малыгина В. Д., Погосян К. А. Рискообразующие факторы инфраструктуры продовольственной системы // Инновационное развитие экономики. 2018. № 4. С. 356—364.

Cyber resilience of food industry enterprises: identifying potential attack vectors

S. Yu. Sidorin, I. G. Blagoveshchensky, E. A. Soboleva

Russian Biotechnology University (ROSBIOOTEKH), Moscow, Russia

V. I. Sharmaev

Moscow Aviation Institute (National Research University), Moscow, Russia

This article presents a study that aims to identify critical network services of a food manufacturing facility and assess the possible consequences of successful attacks on those services. The study was conducted using a simulated environment and network scanning tools to assess the overall cyber resilience of the network. A Mininet network emulator was chosen as the research environment, and the Nmap network scanning tool was used to identify devices on the network and find open ports. The network topology, consisting of 22 hosts and 4 switches, represents the different departments of a flour mill: production department, logistics department, sales department, and human resources department. The main takeaway from the experiment is that an attacker could identify all devices on the network and perform a full scan of all open ports on each device, potentially revealing weaknesses in the network. By investigating specific departments within a flour mill infrastructure, the authors identify possible network services that could be used to perform their respective business functions and analyze the potential consequences of exploiting vulnerabilities and a cyberattack on each. The study provides insight into potential attack vectors on food businesses, highlighting areas that require attention to improve network cyber resilience.

Keywords: cyber resilience, information security, network intelligence, Mininet, Nmap.

Bibliography — 35 references.

Received May 31, 2023

Алгоритм интерливинга распределённого общего кэша многоядерного процессора для произвольного количества банков

Ю. А. Недбайло, А. В. Сурченко
АО «МЦСТ», Москва, Россия

В. А. Пиков

Московский авиационный институт (национальный исследовательский университет), Москва, Россия

Разработан алгоритм интерливинга кэша, поддерживающий произвольное количество банков. Эксперименты на 40-, 48- и 56-ядерных моделях процессора в тестах SPEC CPU2017 показали преимущество предложенного алгоритма над традиционным алгоритмом на основе деления в среднем порядка 1 процента производительности процессора.

Ключевые слова: микропроцессор, многоядерный процессор, кэш память, интерливинг.

В последнее десятилетие производительность процессоров общего назначения значительно повышалась за счёт увеличения количества их ядер. Обычные настольные процессоры сегодня имеют до 16 ядер. При добавлении «энергоэффективных» число ядер и их результирующая производительность становятся ещё больше. Также перспективным направлением повышения вычислительной мощности считается добавление специализированных ядер [1]. В то же время, используемая ими память DRAM развивается не так быстро, поэтому разработчикам процессоров следует искать пути уменьшения времени доступа и частоты обменов с памятью.

Реализация иерархии кэшей, включающей общий кэш, является обычным подходом к этой проблеме; при большом количестве ядер общий кэш делают распределённым с доступом через накрystalную сеть, и для упрощения проектирования количество банков часто делают соответствующим количеству ядер [2]. При этом, из-за особенностей технологии производства микросхем, зачастую оказывается удобным располагать на кристалле количество ядер не являющееся степенью двойки. Кроме того, неко-

торые банки кэша процессоров могут иметь технологические дефекты, не позволяющие их использовать. В таких случаях количество банков кэша, которые можно использовать, не является степенью двойки, и тогда для эффективной работы с кэшем необходим алгоритм вычисления номера банка, индекса и тэга кэш-строки, более сложный, чем традиционное использование просто соответствующих разрядов её адреса.

В данной работе предлагается такой алгоритм, разработанный с целями обеспечить равномерное использование банков кэша без значительного увеличения времени доступа и времени промаха в кэш, и возможность программного отключения дефектных банков. Эксперименты на 40-, 48- и 56-ядерных моделях процессора в тестах SPEC CPU2017 показали преимущество предложенного алгоритма над традиционным алгоритмом на основе деления в среднем порядка 1 процента производительности процессора.

Материалы и методы

Тестовая конфигурация. Предметом данного исследования будет 16-ядерный процессор общего назначения архитектуры Эльбрус шестого поколения, и его модель на основе трасс событий, в которой количество ядер и банков общего кэша будет увеличиваться до 40, 48 или 56. Методика моделирования, описанная в [3], была обновлена до используемой версии архитектуры, её точность была улучшена.

Моделируемые конфигурации приведены в табл. 1.

Недбайло Юрий Александрович, ведущий инженер.
E-mail: yuri.nedbailo@mail.ru

Сурченко Александр Викторович, старший инженер.
E-mail: Alexander.V.Surchenko@mcst.ru

Пиков Виталий Александрович, старший преподаватель кафедры 402 «Радиосистемы и комплексы управления, передачи информации и информационная безопасность».
E-mail: pikov@ya.ru

Статья поступила в редакцию 30 августа 2023 г.

© Недбайло Ю. А., Сурченко А. В., Пиков В. А., 2023

Таблица 1

Конфигурации процессора, используемые при моделировании

Компонент	Конфигурация
Ядро	40/48/56 ядер, Эльбрус v6 @ 2000 МГц
L1i кэш	Приватные, 128 КБ на ядро, 4-way, 256 Б строка
L1d кэш	Приватные, 64 КБ на ядро, 4-way, 32 Б строка
L2 кэш	Приватные (неинклюзивные), 1 МБ на ядро, 4-way, 64 Б строка
L3 кэш	Общий (NCID, FLEXclusion), 2 МБ на ядро, 16-way, 64 Б строка
Накристалльная сеть	Ячеистая 8x5/8x6/8x7, 1 запрос + 32 Б данных за такт на канал
Память	8 каналов, DDR4 @ 3200 MT/c

Главным объектом исследования является распределённый общий L3 кэш, состоящий из 40 / 48 / 56 банков по 2 МБ, и доступ в него со стороны ядер через накристалльную сеть. В результате ранее сделанных и предложенных оптимизаций, кэши реализуют неинклюзивную схему с инклюзивным справочником (NCID) и вариантом оптимизации FLEXclusion [4, 5]. Доступ в общий кэш осуществляется через накристалльную сеть ячеистой (mesh) топологии, организованную как массив «плиток» (tile), содержащих одно ядро и один банк кэша; восемь каналов оперативной памяти

(MC) подключены к краям массива (рис. 1). Каждый пакет передаётся между ближайшими «плитками» за два процессорных такта, из-за чего время доступа в кэш и оперативную память зависит от соответствия адресов кэш-строк банкам кэша и каналам памяти, т. е. алгоритма интерливинга.

Существующие методы. В традиционном кэше с количеством банков и наборов, являющимися степенью двойки, как правило используется интерливинг и индексирование по младшим разрядам адреса строки, и они просто берутся из её адреса, а старшая его часть хранится в кэше как тэг:

$$b = A[\text{offset} + N - 1 : \text{offset}],$$

$$\{tag, idx\} = A[MSB : \text{offset} + N],$$

где b — номер банка; idx и tag — индекс и тэг; MSB — старший разряд адреса A , а $offset$ и N соответствуют размеру кэш-строки (2^{offset} байт) и количеству банков ($2^N = \text{banks}$).

При произвольном количестве банков можно использовать аналогичные формулы, в которых роль младшей и старшей части адреса выполняют остаток от деления и результат деления на количество банков:

$$b = A[MSB : \text{offset}] \% \text{banks},$$

$$\{tag, idx\} = A[MSB : \text{offset}] / \text{banks}.$$

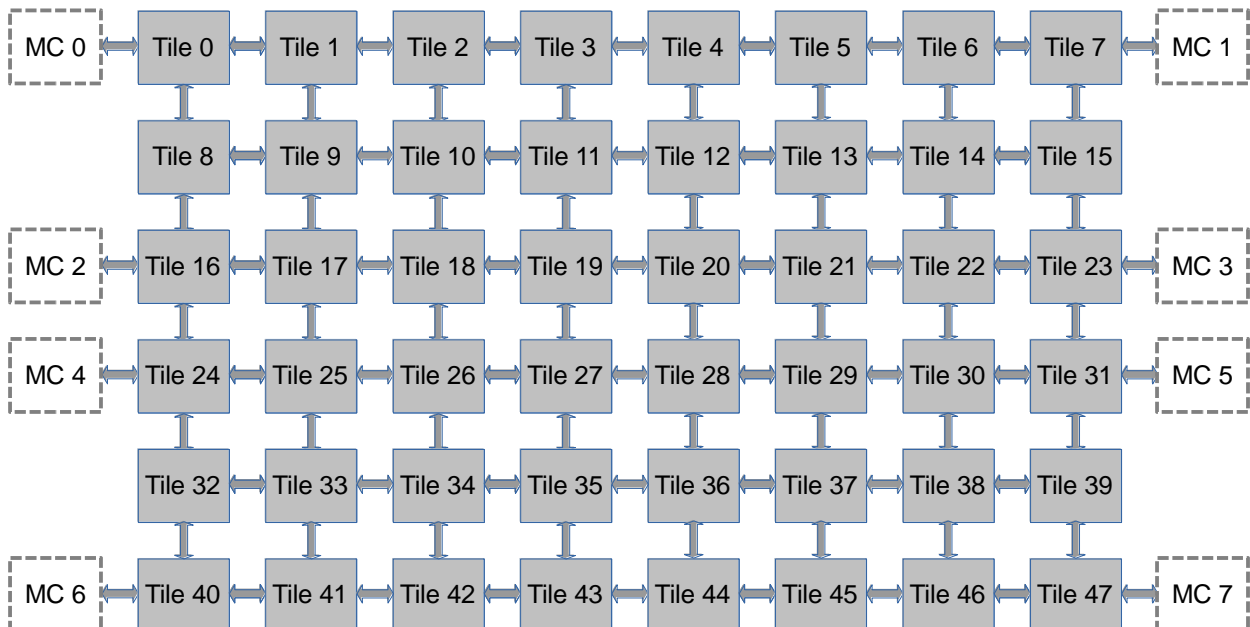


Рис. 1. Топология соединения «плиток» (содержащих одно ядро и один банк кэша) и каналов памяти (MC) в 48-ядерной конфигурации процессора

К сожалению, деление и вычисление остатка — вообще говоря сложные операции, и их использование соответственно может заметно увеличить время доступа в кэш. Даже если применять оптимизации вроде умножения на обратную делителю величину [6], достаточно большая длина физического адреса строки в современных системах делает эту прибавку существенной. Однако, помимо степеней двойки — 2, 4, 8 и т. д. — на которые деление осуществляется тривиальным образом, на числа вида $(2^k - 1)$ или $(2^k + 1)$, например 3, 5, 7, 9, оно также может быть реализовано достаточно быстрым [7]. Таким образом, поскольку деление можно производить в два этапа, достаточно удобными являются все делители вида $2^n \cdot (2^k \pm 1)$, включая все от 2 до 10, и при проектировании процессора — выборе количества каналов памяти и банков кэша — это обычно учитывают, что не сильно ограничивает этот выбор.

Не вполне однозначным при этом является вопрос, нужно ли преобразовывать адрес, хранящийся в банке кэша, то есть индекс и тэг, делением по формуле выше. Известно, что делать это не обязательно, и на равномерность использования наборов кэша это не влияет [8]. С одной стороны, деление по формуле выше уменьшает размер тэга и соответственно количество оборудования, требуемое для их хранения. С другой стороны, если оно производится на входе кэша, тогда как номер банка вычисляется на выходе ядра, время этого преобразования добавляется к времени доступа.

Задачу дополнительно усложняет наблюдение, что и номер банка, и индекс полезно дополнительно преобразовывать, например подмешивая к ним более старшие разряды адреса. За счёт этого достигается более равномерное использование банков и наборов кэша и снижается частота промахов [5]. Существуют различные хэш-функции, предназначенные для этого [9—11], однако диапазон и их аргументов, и значений являются степенями двойки, поэтому для интерливинга в обсуждаемом случае они напрямую не применимы.

Основные цели и идеи при разработке алгоритма. Специфика применения алгоритма интерливинга в распределённом общем кэше универсального процессора продиктовала следующие цели, которые преследовались при его разработке:

1. Возможность программного отключения как минимум одного банка.
2. Равномерность распределения адресов по банкам.
3. Минимальный размер тэгов, если преобразовывать индекс и тэг.
4. Минимальное время доступа и промаха в кэш.

Из этих целей и известных существующих методов, их достоинств, недостатков и ограничений, вытекают следующие идеи, легшие в основу метода.

Первая идея — поделить банки на группы, как показано на рис. 2.

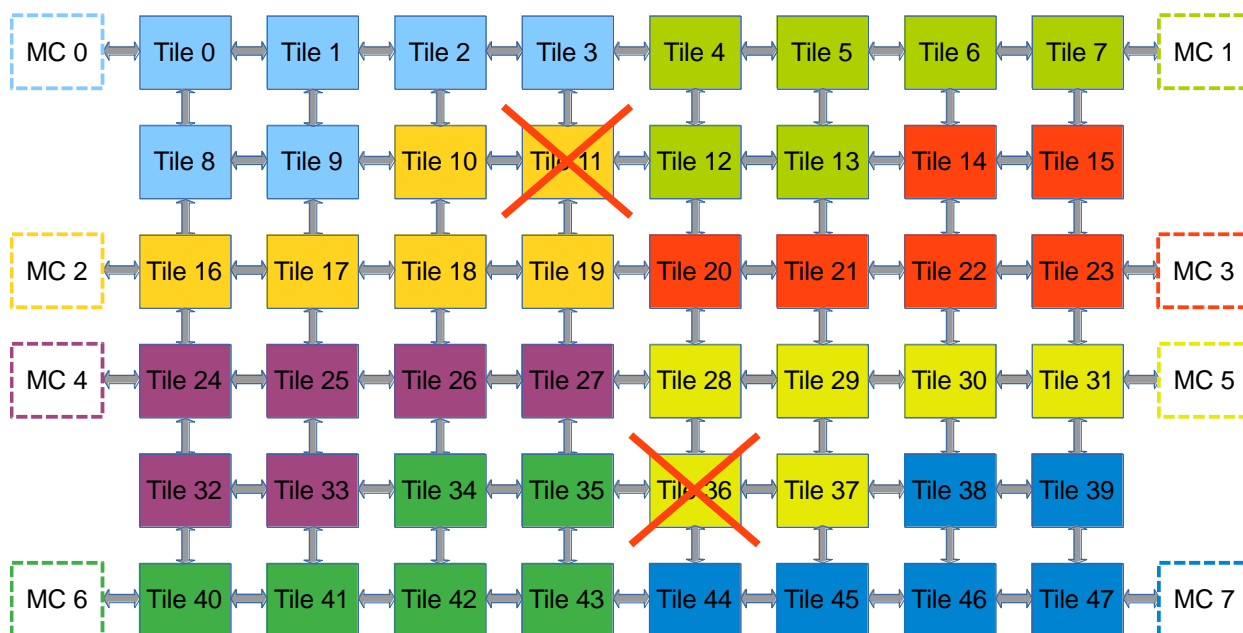


Рис. 2. Деление банков кэша на группы, соответствующие каналам памяти, и возможное отключение банков в 48-ядерной конфигурации процессора

С одной стороны, как уже говорилось в предыдущем параграфе, достаточно удобно выбирать количества банков представимое в виде $2^n \cdot (2^k \pm 1)$. С другой стороны, для минимизации времени доступа в память важно привязать каждый банк кэша к ближайшему каналу памяти. В универсальных процессорах количество каналов памяти чаще всего является небольшой степенью двойки, и в этом случае число банков в группе будет также удобного вида $2^m \cdot (2^k \pm 1)$. Но даже если и не является, скорее всего можно на этапе выбора количества банков согласовать их соответствующим образом.

Вторая идея — возможность отключения одного банка в каждой группе. Дефекты в кэше чаще всего возникают в его памяти состояний или тэгов, и такие дефекты можно обходить, помечая соответствующие позиции в кэше как неиспользуемые. Соответственно, отключение всего банка требуется сравнительно редко. Если сделать отключаемым один банк в каждой группе, этого будет скорее всего достаточно даже для отключения двух банков в процессоре — если они в разных группах. Например, при 8 группах банков, процессор с двумя дефектными будет пригоден к использованию в 87,5 % случаев.

Третья идея — деление части адреса, а не всего адреса, с подмешиванием хэша от остальных разрядов адреса. Деление всего адреса на какое-то число не обеспечивает хорошей равномерности распределения обращений по банкам поскольку в некоторых задачах некоторые обращения будут идти с шагом, соответствующим такому интерливингу. Деление части адреса в этом смысле не сильно лучше, но оно занимает меньше времени, и к его остатку можно, как будет показано далее, подмешивать хэш от остальных разрядов таким образом, чтобы достигались цели 2, 3 и 4.

Четвёртая идея — преобразовывать индекс и тэг соответствующим вычислению номера банка образом, а время этого и обратного преобразования скрывать некоторыми оптимизациями кэша и накристалльной сети.

Разработанный алгоритм. Как показано на рис. 2 для случая 48 банков кэша и 8 каналов оперативной памяти, все банки разделены на группы, соответствующие ближайшему каналу памяти. Предполагая количество каналов являющимся степенью двойки, номер группы вычисляется из адреса кэш-строки достаточно традиционным способом — берутся несколько разрядов адреса и к ним операцией XOR подмешиваются остальные разряды по некоторой матрице. Для случая на рис. 2:

$$g[0] = A[il_bit0] \wedge (\wedge (A[MSB:offset] \& mask0)),$$

$$g[1] = A[il_bit1] \wedge (\wedge (A[MSB:offset] \& mask1)),$$

$$g[2] = A[il_bit2] \wedge (\wedge (A[MSB:offset] \& mask2)),$$

где $g[i]$ — i -й бит номера группы, $il_bit0...il_bit2$ ($> offset$) — настраиваемые номера битов, $mask0...mask2$ для экспериментов выбраны согласно интерливингу «shift» в [5].

Для дальнейших вычислений используется адрес A_p , из которого биты $il_bit0...il_bit2$ "выколоты", т. е. все биты адреса с номером il_bit0 и выше заменены операцией сдвига битами $(il_bit0 + 1)$ и так далее. Использовать и хранить эти биты на следующих этапах алгоритма и в кэше не нужно, потому что они высстраиваются из A_p и g по формулам, аналогичным вышеуказанным:

$$A[il_bit0] = g[0] \wedge (\wedge (A_p[MSB:offset] \& mask0')),$$

$$A[il_bit1] = g[1] \wedge (\wedge (A_p[MSB:offset] \& mask1')),$$

$$A[il_bit2] = g[2] \wedge (\wedge (A_p[MSB:offset] \& mask2')),$$

где $mask0' ... mask2'$ — те же маски, что и выше, но с учётом «выкалывания».

Вычислив из полного адреса A номер группы, по сути остаётся вычислить из A_p номер банка внутри этой группы b_g ; в иллюстрируемом случае он может принимать шесть или, если один из банков этой группы отключен, пять значений. Идея использовать остаток от деления части разрядов адреса уже объяснялась; способ подмешивать к нему хэш от остальных разрядов был выбран экспериментально. Итоговая формула:

$$b_g = \left(A_p \left[\begin{array}{l} il_bit3 + \\ +D-1 : il_bit3 \end{array} \right] \% G[g] + \right. \\ \left. + hash(A_p) \right) \% G[g],$$

где il_bit3 и D задают диапазон разрядов, используемых для деления; $G[g]$ — количество активных банков в группе; $hash$ — четырёхразрядный XOR-хэш от более старших разрядов адреса, аналогичный «shift» в [5]. Эта формула, впрочем, определяет номер банка среди активных. Для получения «физического» номера его нужно скорректировать:

$$b_g' = ((b_g < dis[g]) ? b_g : b_g + 1),$$

где $dis[g]$ — номер отключенного банка (достаточно большой, если отключенных нет).

Номер банка вычисляется из номера группы g и номера банка внутри группы b_g' в соответствии с топологией процессора. Рис. 2 соответствует:

$$b[2] = g[0],$$

$$\{b[5:3], b[1:0]\} = G \cdot g[2:1] + b_g',$$

где G – физическое количество банков в группе (в данном случае 6).

Аппаратная реализация. Приведённый алгоритм содержит ряд операций, не относящихся к простым. Высокая скорость его реализации в процессоре достигается параллельным их выполнением и небольшой разрядностью операндов. Вычисление b_g и b_g' показано на рис. 3. Здесь b_g вычисляется сразу в двух вариантах, чтобы деление производилось на константу. Параллельно производится вычисление g , представляющее собой ряд операций XOR, и затем умножение g на G . Критическим путём такой схемы будет показанная на рис. 3 логика плюс, в конце, сложение и, если биты интерливинга — программируемые, дополнительные операции сдвига вначале.

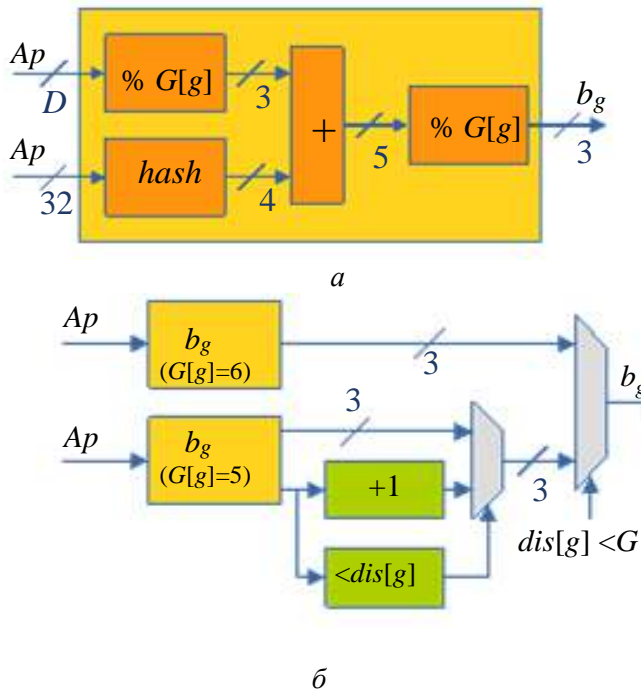


Рис. 3. Аппаратная реализация вычисления:

$$a - b_g ; б - b_g'$$

Универсальность. Если количество каналов памяти не является степенью двойки, вычислять g и A_p можно обычным делением всего адреса. Это

увеличит время работы алгоритма, но представляется неизбежным при привязке банков кэшa к ближайшему каналу памяти. При количестве банков, не кратном количеству каналов памяти, алгоритм может быть использован в описанном виде с поправками на то, что количество банков в разных группах будет отличаться. Таким образом предложенный алгоритм применим при любом количестве каналов памяти и банков кэшa, но в описанном случае 2^m и $2^n \cdot (2^k \pm 1)$, соответственно, где $m \leq n$, он обеспечит наилучшую скорость.

Преобразование индекса и тэга. Как и в случае с использованием обычного остатка от деления адреса в качестве номера банка, при описанном алгоритме интерливинга специальное преобразование адреса для использования его внутри кэшa, в принципе, не требуется — только «выкалывание» некоторых разрядов. Но если в традиционном случае такое преобразование — деление на количество банков — только уменьшает размер тэгов и не влияет на эффективность работы кэшa (что было проверено экспериментально), в случае предложенного алгоритма оно повышает и эффективность.

Аналогичным делению в данном случае является следующее преобразование:

$$\{tag, idx\} = A_{L3} =$$

$$= (A_p[il_bit3 + D - 1 : il_bit3] / G[g]) +$$

$$+ M[g] \cdot A_p[MSB : il_bit3 + D],$$

где $M[g] = \lceil 2^D / G[g] \rceil$ соответствует количеству значений, принимаемых результатом деления, и зависит от D и количества банков в группе как показано в табл. 2. Из неё видно, что $D = 5$ является очень удобным, поскольку при любом количестве банков кроме трёх, $M[g]$ будет числом, делить на которое достаточно легко.

Таблица 2

Зависимость $M[g]$ от D и $G[g]$

	$D = 5$	$D = 6$	$D = 7$	$D = 8$	$D = 9$
$G[g] = 3$	11	22	43	86	171
$G[g] = 4$	8	16	32	64	128
$G[g] = 5$	7	13	26	52	103
$G[g] = 6$	6	11	22	43	86
$G[g] = 7$	5	10	19	37	74
$G[g] = 8$	4	8	16	32	64

Естественно, преобразовывать адрес в кэше можно только таким образом, чтобы из преобразованного адреса, номера банка и параметров интерливинга можно было восстановить исходный адрес. Для этого получаются следующие формулы:

$$A_p[il_bit3 + D - 1 : il_bit3] = (A_{L3} \% M[g]) \cdot G[g] + (b_g - \text{hash}(A_{L3} / M[g])) \% G[g],$$

$$A_p[MSB : il_bit3 + D] = A_{L3} / M[g].$$

Оба преобразования, прямое и обратное, сравнительно сложные, поэтому их стоит реализовывать вместе с двумя достаточно простыми оптимизациями.

Аппаратные оптимизации преобразования. При доступе в кэш, индекс нужен в первую очередь: для чтения состояний и тэгов кэш-строк соответствующего набора. Он достаточно небольшой — 11 бит в рассматриваемом процессоре — и его вычисление похоже на вычисление номера банка: та же часть адреса делится на то же число активных банков, и к результату подмешиваются несколько более старших разрядов (в том числе, при использовании хэш-функций для индексирования). Первой оптимизацией, соответственно, будет вычисление индекса одновременно с номером банка и передача его по сети вместе с запросом в кэш. Это показано на рис. 4 слева. Тэг можно вычислять в самом кэше во время считывания нужного набора.

Обратное преобразование — восстановление адреса из индекса, тэга и номера банка — нужно в разных случаях, например *writeback* или *snoor*-запросов, но его скорость критична только для запросов чтения, промахнувшихся в кэш и отправляемых в память. Причём оно вполне проявляет себя только когда запрос сразу идёт на выход, без блокировок. Второй оптимизацией соответственно будет передача исходного адреса запроса на выход кэша через его конвейер, чтобы адрес сразу использовался для формирования запроса в память при промахе в кэш, без задержек на преобразование. В остальных случаях можно потратить несколько тактов на восстановление адреса по формулам из предыдущего параграфа без заметного ущерба для производительности, поскольку на время доступа в память эти задержки не повлияют.

С такими оптимизациями алгоритм можно будет эффективно использовать при разных сочетаниях количества банков и параметра D ; в частности, при «удобном» количестве банков $2^n \cdot (2^k \pm 1)$, параметр D можно выбирать достаточно большим.

Результаты

Средняя производительность (IPC) в тестах пакета SPEC CPU2017 *refrate* в зависимости от алгоритма интерливинга и преобразования адреса внутри кэша на 40-, 48- и 56-ядерных моделях процессора показана на рис. 5.

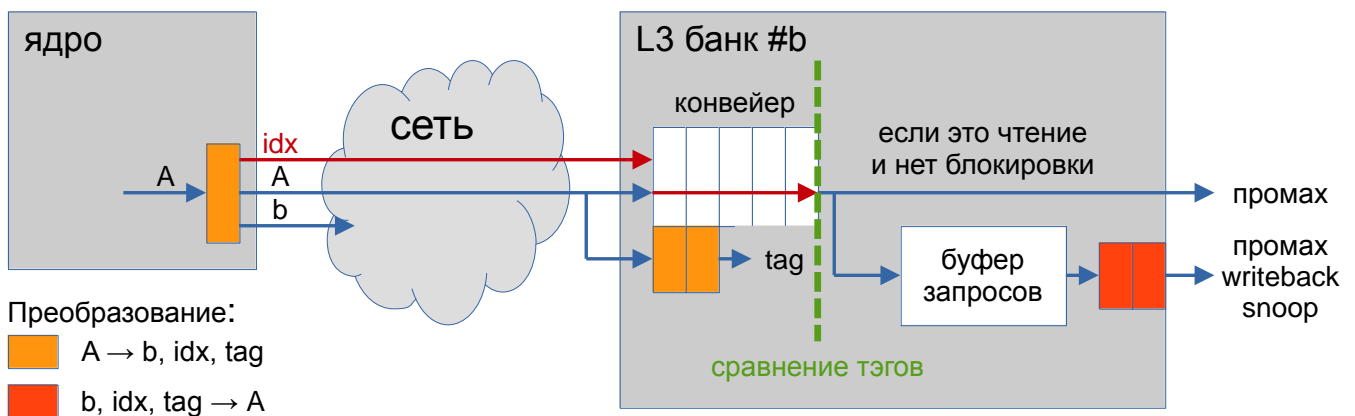


Рис. 4. Аппаратные оптимизации преобразования индекса и тэга

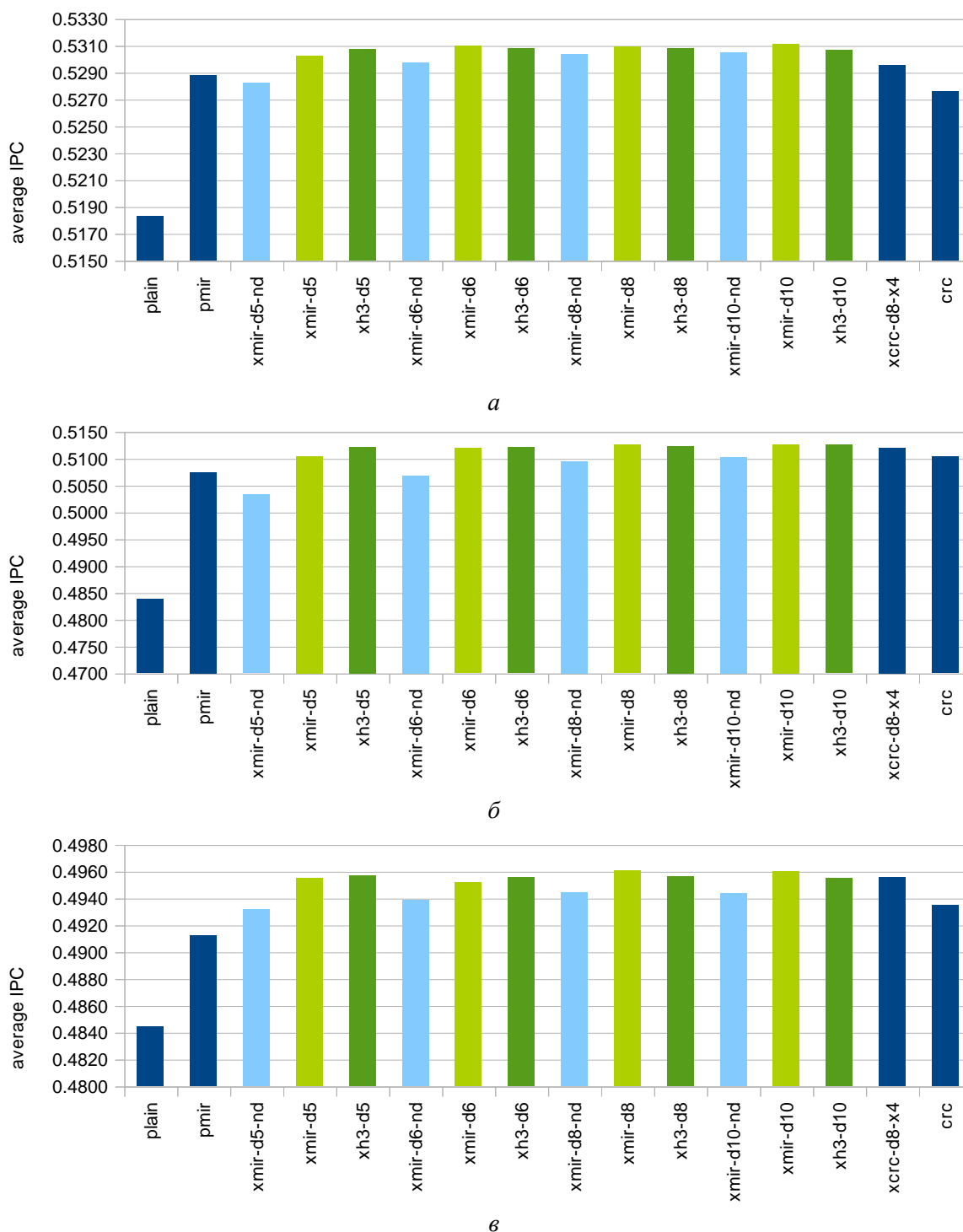


Рис. 5. Средняя производительность в тестах SPEC CPU2017 refrate:
а — 40-; б — 48-; в — 56-ядерных моделях процессора

Первые два столбца (*plain*, *pmir*) соответствуют традиционному вычислению номера банка как остатка от деления адреса на количество банков; второй столбец (*pmir*) при этом подразумевает подмешивание в индекс младшей части тэга аналогично индексированию "*mir*" в [5]; более сложное индексирование при таком алгоритме интерливинга наверняка увеличит время доступа в кэш

и потому не рассматривалось. Последние два столбца (*crc*, *xcrc-d8-x4*) выполняют роль эталона, представляя модификации обсуждаемых алгоритмов с использованием хэш-функции CRC32.

Столбцы *xmir-dX-nd* обозначают базовый вариант алгоритма с разными значениями параметра *D*, в котором преобразование индекса и тэга не осуществляется, но внутри кэша используется индекс

сирование "mir". Уже при $D = 8$ этот алгоритм показывает результаты на 0,30 % / 0,39 % / 0,65 % лучшие, чем традиционный с таким же "mir"-индексированием, для 40/48/56 ядер и банков, при том что не более сложен в реализации.

Столбцы *xmir-dX* и *hx3-dX* соответствуют варианту алгоритма с преобразованием и оптимизациями, и отличаются индексированием "mir" в первом случае и более сложным «*h3*» из [5] во втором. Первый вариант при $D = 10$ достигает преимущества в 0,44 % / 1,02 % / 0,97 % для 40/48/56 ядер и банков. Второй вариант демонстрирует близкие результаты — 0,37 % / 0,92 % / 0,91 % — уже при $D = 5$, что позволяет ожидать достаточно быстрой его работы несмотря на сложное индексирование, поскольку оптимизации подразумевают вычисление индекса одновременно с номером банка.

Приведённые результаты получены при работе всех ядер, и их разница обусловлена в основном разницей в частоте промахов в кэш. При работе одного или небольшого количества ядер можно было бы ожидать другую картину, обусловленную разной степенью разброса времени доступа из-за разного распределения адресов по банкам; традиционное деление должно обеспечивать наименьший разброс, а использование хэш-функций — увеличивать его. Это предположение было проверено; при одном активном ядре средняя разница производительности составила десятые доли процента и была в пользу алгоритмов, использующих хэш-функции.

Заключение

Распределённый общий кэш часто реализуется в многоядерных процессорах общего назначения. Особенности производства процессоров иногда приводят к тому, что количество используемых банков этого кэша не является степенью двойки. Для таких случаев был разработан алгоритм интерливинга кэша и несколько его оптимизаций.

Сам интерливинг, то есть вычисление номера банка по адресу кэш-строки, в предложенном алгоритме осуществляется путём разделения банков на группы, соответствующие каналам памяти, и затем вычисления номера банка внутри группы. Для последнего, к остатку от деления части разрядов адреса на количество банков в группе прибавляется простая хэш-функция от других разрядов адреса.

Оптимизациями, минимизирующими размер хранимых в кэше тэгов и время доступа и промаха в кэш, являются преобразование хранимого в кэше

адреса и скрывание задержек на это преобразование. Индекс и тэг преобразуется таким образом, чтобы исходный адрес можно было восстанавливать из них, номера банка и параметров интерливинга. Индекс вычисляется одновременно с вычислением номера банка и передаётся по накрестальной сети вместе с запросом в кэш. В кэше, тэг вычисляется одновременно с чтением состояний и тэгов запрашиваемого набора, а исходный адрес запроса передаётся через конвейер до места формирования запроса в память.

В экспериментах на 40-, 48- и 56-ядерных моделях, базовый вариант алгоритма демонстрирует сравнимую или чуть лучшую производительность в зависимости от параметров реализации по сравнению с традиционным алгоритмом на основе полного деления адреса. Со всеми оптимизациями, алгоритм показывает преимущество порядка 1 процента общей производительности процессора.

Литература

1. *Hennessy John L., Patterson David A.* Computer Architecture, Sixth Edition: A Quantitative Approach. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 6th edition, 2017.
2. *Iyer R., De V., Illikkal R. et al.* Advances in Microprocessor Cache Architectures Over the Last 25 Years // IEEE Micro. 2021. V. 41, № 6. P. 78—88.
3. *Nedбайло Yu.* Fast and scalable simulation framework for large in-order chip multiprocessors. In 2020 26th Conference of Open Innovations Association (FRUCT), 2020. P. 335—345.
4. *Sim J., Lee J., Qureshi M. K., Kim H.* FLEXclusion: Balancing cache capacity and on-chip bandwidth via flexible exclusion. SIGARCH Comput. Archit. News, 40(3):321—332, June 2012.
5. *Недбайло Ю. А., Сурченко А. В., Бычков И. Н.* Снижение частоты промахов в инклюзивный кэш с инклюзивным справочником многоядерного процессора // Компьютерные исследования и моделирование. 2023. Т. 15. № 3. С. 639—656.
6. *Daniel Lemire, Colin Bartlett, & Owen Kaser* (2021). Integer division by constants: optimal bounds. Heliyon, 7(6), e07442.
7. *De Dinechin, B. D.* (1991, August). A ultra fast Euclidean division algorithm for prime memory systems. In Proceedings of the 1991 ACM/IEEE conference on Supercomputing (pp. 56—65).
8. *Seznec A.* Bank-interleaved cache or memory indexing does not require euclidean division // 11th Annual Workshop on Duplicating, Deconstructing and Debunking, Jun 2015, Portland, United States.
9. *Gonzalez A., Valero M., Topham N., Parcerisa J. M.* Eliminating Cache Conflict Misses through XOR-Based Placement Functions // Proceedings of the 11th International Conference on Supercomputing. ICS '97. New York, NY, USA: Association for Computing Machinery, 1997. P. 76—83.
10. *Vandierendonck H., De Bosschere K.* XOR-based hash functions // IEEE Transactions on Computers. 2005. V. 54, № 7. P. 800—812.
11. *Salwan H.* Eliminating Conflicts in a Multilevel Cache Using XOR-Based Placement Techniques // 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing. — 2013. P. 198—203.

An interleaving algorithm for a distributed shared cache of a multi-core processor with an arbitrary number of banks

Yu. A. Nedbailo, A. V. Surchenko

Joint Stock Company «MCST», Moscow, Russia

V. A. Pikov

Moscow Aviation Institute (National Research University), Moscow, Russia

A cache interleaving algorithm has been developed that supports an arbitrary number of banks. Experiments on 40-, 48- and 56-core processor models in SPEC CPU2017 tests showed the advantage of the proposed algorithm over the traditional division-based algorithm by an average of about 1 percent of processor performance.

Keywords: microprocessor, chip multiprocessor, cache memory, interleaving.

Bibliography — 11 references.

Received August 30, 2023

БЛАНК-ЗАКАЗ НА ПОДПИСКУ 2024 г.
на издания ФГУП «НТЦ оборонного комплекса «Компас»

Наименование издания	Индекс издания (количество выпусков в год)	Цена 1 экз., руб.	Кол-во выпусков в год	Общая сумма, руб.
Оборонный комплекс — научно-техническому прогрессу России	4	1600,00		
Конструкции из композиционных материалов	4	1750,00		
Экология промышленного производства	4	1600,00		
Информационные технологии в проектировании и производстве	4	1800,00		
Вопросы защиты информации	4	1800,00		
В цену включены: НДС — 10 % и стоимость почтовой доставки.				

Поставка журналов подписчикам через издательство осуществляется почтовыми бандеролями с приложением всех необходимых бухгалтерских документов.

Наши реквизиты:

Полное наименование организации: _____

Сокращенное наименование организации: _____

ИНН/КПП _____

ОКПО _____

Расчётный счёт № _____ в _____

к/с _____ БИК _____

Юридический адрес: _____

Почтовый адрес: _____

Контактное лицо _____ тел. _____

E-mail: _____

(Для оформления счёта и бухгалтерских документов просьба заполнить все строчки).

Справочно:

Заполненный бланк-заказ просьба отправить по факсу: 8(495) 491-44-80 или

E-mail: secretariat@ntckompas.ru

Более подробную информацию об изданиях и подписке можно получить по телефону:

8 (495) 491-43-17

E-mail: ivleva@ntckompas.ru

Адрес редакции: 125424, Москва, Волоколамское шоссе, д.77.

ФГУП «НТЦ оборонного комплекса «Компас».