ISSN 2225-5435

Вестник УрФО.

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 2(40) / 2021

УЧРЕДИТЕЛИ

ФГАОУ ВО «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ООО «ЮЖНО-УРАЛЬСКИЙ ЮРИДИЧЕСКИЙ ВЕСТНИК»

Подписной индекс 73852 в каталоге «Почта России»

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Свидетельство ПИ № ФС77-65765 от 20.05.2016

Издатель: **ООО «Южно-Уральский юридический вестник»**

Адрес редакции и издателя: Россия, 454080, г. Челябинск, пр. Ленина, д. 76.
Тел./факс (351) 267-97-01.

Электронная версия журнала в Интернете:
www.info-secur.ru,
e-mail: urvest@mail.ru

16+

Journal of the Ural Federal District. Information security

ISSN 2225-5435

№ 2(40) / 2021

FOUNDER

SOUTH URAL STATE UNIVERSITY

SOUTH URAL LEGAL NEWSLETTER

CHAIRMAN OF THE EDITORIAL BOARD

CHUVARDIN O. P.,

Head of Department Federal Service for Technical and Export Control of Russia for the Urals Federal District

CHIEF EDITOR

SOKOLOV A.N.,

Ph.D., Associate Professor, Head of Department "Information Protection", South Ural State University (National Research University) (Chelyabinsk city)

PRODUCING EDITOR

SOGRIN E. K.

LAYOUT

SHRABER A. E.

PROOFREADING

FEDOROV V. S.

Subscription index 73852

in the «Russian Post» catalog

The journal is registered by the Federal service in the field of communication, information technology and mass communications.

Certificate
PI No. ФС77-65765 dd. 05/20/2016

Publisher: OOO « South Ural Legal Newsletter»

Editorial and publisher address: Russia, 454080, Chelyabinsk, Lenin Avenue, 76
Phone / fax (351) 267-97-01.

Electronic version of the magazine in the Internet:

www.info-secur.ru,
e-mail: urvest@mail.ru

16+

В НОМЕРЕ

RESEARCH AND DESIGN OF TECHNICAL FACILITIES

INFORMATION TECHNOLOGY AND COMPUTER SECURITY

METHODS OF DATA ANALYSIS

METHODS OF DATA ANALYSIS

METHODS OF DATA ANALYSIS

УДК 004.056

Вестник УрФО № 2(40) / 2021, с. 5–13

Хорев А.А., Суровенков Д.Б., Савин А.Д.

DOI: 10.14529/secur210201

ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ПОМЕЩЕНИЙ ОТ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ ПО АКУСТООПТИЧЕСКОМУ КАНАЛУ ПУТЕМ УСТАНОВКИ НА ВНЕШНИХ ОКОННЫХ СТЕКЛАХ СВЕТООТРАЖАЮЩИХ ПЛЕНОК

В статье приведены результаты экспериментальных исследований эффективности защиты помещений от утечки речевой информации по акустооптического каналу путем установки на внешних оконных стеклах светоотражающих пленок. В качестве объекта исследований были выбраны солнцезащитные пленки компании Solarblock серии Silver с коэффициентами светопропускания от 0,5% до 47%. При проведении экспериментальных исследований использовались лазерные доплеровские виброметры PDV-100 и RSV-150. Результаты проведенных исследований показали, что при лазерном зондировании жалюзи, установленных внутри помещения, установка на внешних оконных стеклах солнцезащитных пленок с целью защиты помещения от перехвата речевой информации по акустооптического каналу малоэффективна.

Ключевые слова: *акустооптический канал утечки информации, лазерный микрофон, лазерный доплеровский виброметр, защита помещения, солнцезащитные пленки.*

EXPERIMENTAL RESEARCH OF THE EFFECTIVENESS OF PROTECTING PREMISES FROM THE LEAKAGE OF SPEECH INFORMATION THROUGH THE LASER CHANNEL BY INSTALLING REFLECTIVE FILMS ON THE EXTERNAL WINDOW PANES

The article presents the results of experimental research on the effectiveness of protecting premises from the leakage of speech information through the laser channel by installing reflective films on the external window panes. As the object of research, the sun protection window films of Solarblock Silver series with light transmission coefficients from 0.5% to 47% were selected. PDV-100 and RSV-150 laser Doppler vibrometers were used for the aims of experimental research. The results of the conducted research have shown that when laser irradiates the blinds installed indoors, the installation of sun protection window films on the external window panes to protect the room from the interception of speech information through the laser channel is ineffective.

Keywords: *laser channel of speech information leakage, laser microphone, laser Doppler vibrometer, room protection, sun protection window films.*

Одним из наиболее опасных технических каналов утечки акустической речевой информации из защищаемых помещений является акустооптический канал [1]. Перехват акустической речевой информации по данному каналу осуществляется путем лазерного «зондирования» оконных стекол или других отражающих поверхностей, например, оконных штор, жалюзи или различных предметов, установленных в помещении [1-4]. Средства разведки, используемые для перехвата акустической речевой информации по акустооптическому каналу, очень часто называют «лазерными микрофонами» [1].

Для защиты помещений от перехвата акустической речевой информации по акустооптическому каналу используются как активные, так и пассивные средства защиты [2 - 5]. Одними из наиболее доступных и недорогих средств защиты являются солнцезащитные пленки, которые наклеиваются на оконные стекла защищаемого помещения [6].

В работах [2,4] приводятся результаты исследований по использованию солнцезащитных пленок в целях защиты речевой информации от утечки по акустооптическому каналу. Однако, в них не проводилась оценка влияния солнцезащитных пленок на разборчивость речи в случае лазерного «зондирования» жалюзи, установленных на окнах внутри защищаемого помещения.

Целью данной работы являются экспери-

ментальные исследования эффективности светоотражающих пленок, устанавливаемых на внешних оконных стеклах, при защите речевой информации от ее перехвата по акустооптическому каналу при лазерном «зондирования» жалюзи, установленных на окнах защищаемого помещения.

В качестве объекта исследований были выбраны солнцезащитные пленки компании Solarblock серии Silver, коэффициенты светопропускания которых приведены в таблице 1 [6].

закреплен двухкамерный стеклопакет (рисунок 1б). На внешнюю оконную поверхность стеклопакета были наклеены 7 фрагментов солнцезащитных пленок размером 70 × 70 мм (3), коэффициенты светопропускания которых приведены в таблице 1. С тыльной стороны оконного блока была установлена непрозрачная, светорассеивающая тканевая жалюзи (1), на которую в нескольких местах были закреплены фрагменты световозвращающей пленки 3M Scotchlite серии 983, размерами 7 × 7 мм (2).

Таблица 1

Коэффициент пропускания видимого света солнцезащитных пленок

Тип пленки	Коэффициент светопропускания в видимом диапазоне, %	Коэффициент светопропускания в инфракрасном диапазоне, %
Silver 40	47	31
Silver 25	29	28
Silver 15	20	20
Silver 5	7	7
Silver 25 + Silver 5	2	2
Silver 15 + Silver 5	1,5	1,4
Silver 5 + Silver 5	0,5	0,5

Примечание: Значения коэффициентов светопропускания в ИК диапазоне приведены на основе оценочных данных производителя.

Для проведения экспериментальных исследований был создан лабораторный испытательный стенд (рисунок 1а), в состав которого входили: 1 – подкатная стойка CP-022-02 ESD; 2 – лазерный доплеровский виброметр; 3 – шумомер-вибромер «Экофизика-110А»; 4 – генератор сигналов AGILENT 33210A; 5 – акустическая колонка «Behringer EUROLIVE B208D»; 6 – ноутбук.

На подкатной стойке CP-022-02 ESD был

Для формирования тестового акустического сигнала использовалась акустическая колонка «Behringer EUROLIVE B208D» и генератор сигналов AGILENT 33210A. В качестве тестового сигнала использовался «белый» шум.

В качестве модели «лазерного микрофона» использовались лазерные доплеровские виброметры PDV-100 и RSV-150, основные характеристики которых приведены в таблице 2.

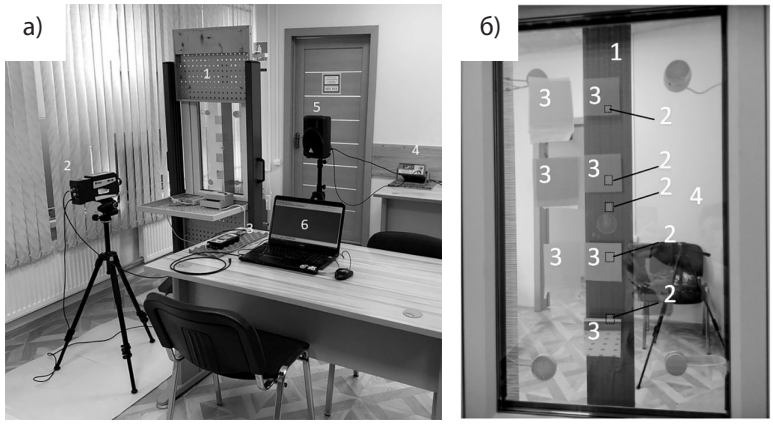

Рисунок 1 – Лабораторный стенд для исследования эффективности солнцезащитных пленок: общий вид (а); схема установки фрагментов солнцезащитных пленок на оконном блоке (в)

Таблица 2

Технические характеристики лазерных доплеровских виброметров PDV-100 и RSV-150

Наименование характеристики	Значение характеристики	
	PDV-100	RSV-150
Класс лазера	2	2
Тип лазера	HeNe	HeNe
Длина волны, мкм	~ 0,63	1,55
Мощность лазера, мВт	0,6	10
Минимальное/максимальное рабочее расстояние, м	0,1 – 30	5 – 300
Диапазон частот, Гц	0,5 – 22 000	0 – 25 000
Разрешающая способность по скорости, мкм/с/√Гц	<0,02	< 0,5

Для измерения уровня вибрационного сигнала, возбуждаемого тестовым акустическим сигналов на ламели жалюзи, использовался шумомер-виброметр «Экофизика-110А». Шумомер-виброметр подключался к аналоговому выходу лазерного виброметра.

Ноутбук использовался для обработки результатов измерений.

При проведении экспериментальных исследований лазерным излучением облучались матерчатые ламели жалюзи, установленные за стеклопакетом. При этом лазерный луч проходил через фрагмент солнцезащитной пленки, наклеенный на внешнее оконное стекло стеклопакета.

Исследования проводились в два этапа. На первом этапе лазерным лучом обучались фрагменты световозвращающих пленок, закрепленные на матерчатой ламели жалюзи (зеркальное отражение), а на втором этапе – облучалась непосредственно поверхность ламели (диффузное отражение).

В качестве показателя оценки эффективности светоотражающих пленок использовалась словесная разборчивость речи (W), которая рассчитывалась на основе результатов измерений отношений сигнал/шум в октавных полосах на выходе лазерного виброметра.

Измерения отношений сигнал/шум при использовании лазерного доплеровского виброметра PDV-100 (видимый диапазон длин волн) проводились в следующей последовательности:

– лазерный виброметр устанавливался на 1 м от внешнего стекла оконного блока. Для исключения влияния диффузного отражения солнцезащитной пленки на результаты измерений, ось виброметра направлялась на стекло (в точке установки пленки) под углом $\beta = 20^0$;

– производилась юстировка и фокусировка оптической системы лазерного луча виброметра на поверхности ламели, так чтобы луч лазера проходил сквозь фрагмент солнцезащитной пленки;

– звуковая колонка устанавливалась на расстоянии 1 м от внутреннего стекла оконного блока. На расстоянии 1 м от звуковой колонки устанавливался измерительный микрофон, подключенный к шумомеру. С генератора сигналов на вход звуковой колонки подавался тестовый сигнала в виде «белого шума» и с помощью шумомера измерялось звуковое давление тестового сигнала в 7-ми октавных полосах (L_{si}, где i =1…7);

– шумомер-виброметр подключался к аналоговому выходу лазерного виброметра и при включенном тестовом сигнале проводились измерения уровня вибрационного сигнала на выходе лазерного виброметра в 7-ми октавных полосах (V_{si}, где i=1…7);

– тестовый сигнал выключался и проводились измерения уровня вибрационного шума на выходе лазерного виброметра в 7-ми октавных полосах (V_n, где i=1…7).

Измерения отношений сигнал/шум при использовании лазерного доплеровского виброметра RSV-150 (инфракрасный диапазон длин волн) проводились аналогично, но при этом для исключения влияния диффузного отражения солнцезащитной пленки на результаты измерений, ось виброметра направлялась на стекло (в точке установки пленки) под углом $\beta = 40^0$, а исследуемая поверхность располагалась на расстоянии не 1 м, а 15 м от измерительной головки лазерного виброметра.

Далее проводился расчет уровней скрываемого вибрационного сигнала (V_{ci}) и отношений сигнал/шум (q_i) в 7-ми октавных полосах по формулам [1]:

$$V_{\text{с},i} = 10\lg(10^{0,1V_{\text{и},i}-0,1V_{\text{ш},i}}) - \left(L_{\text{и},i} - L_{\text{с},i}\right); \quad (1)$$

$$q_i = V_{\text{с},i} - V_{\text{ш},i}, \quad (2)$$

где L_{ci} – акустическое давление, соответству-

ющее среднему уровню громкости речи в i – ой октавной полосе (см. таблицу 3).

Измерения проводились для каждого типа пленки.

Для расчета словесной разборчивости речи (W) использовалась методика, в основу которой положен форматный метод оценки разборчивости речи [1]:

$$Q_i = q_i - \Delta A_i; \quad (3)$$

$$p_i = \begin{cases} \dfrac{0{,}78 + 5{,}46\exp[-4{,}3\cdot 10^{-3}(27{,}3 - |Q_i|)^2]}{1 + 10^{0{,}1|Q_i|}}; \\ \text{если } Q_i \le 0, \\ 1 - \dfrac{0{,}78 + 5{,}46\exp[-4{,}3\cdot 10^{-3}(27{,}3 - |Q_i|)^2]}{1 + 10^{0{,}1|Q_i|}}; \\ \text{если } Q_i > 0, \end{cases} \quad (4)$$

$$R_i = p_i \kappa_i; \quad (5)$$

$$R = \sum_{i=1}^{7} R_i; \quad (6)$$

$$W = \begin{cases} 1{,}54R^{0{,}25}[1 - \exp(-11R)], \text{если } R < 0{,}15; \\ 1 - \exp\left(\dfrac{-11R}{1 + 0{,}7R}\right), \text{если } R \ge 0{,}15, \end{cases} \quad (7)$$

где ΔA_i – значение формантного параметра речи в i-й октавной полосе, дБ;

k_i – весовой коэффициент i-й октавной полосы.

Характеристики октавных полос, используемые при расчете по данной методики, приведены в таблице 3 [1].

Результаты измерений, проведенных в соответствии с методикой, приведены в таблицах 4 и 5.

Рассчитанные значения разборчивости речи W приведены в таблицах 6 и 7.

Анализ данных, представленных в таблицах 6 и 7, показал, что:

а) при зеркальном отражении лазерного

Таблица 3

Характеристики октавных полос

№	Среднегеометрическая частота f_i, Гц	Типовые уровни речи L_{ci}, дБ	Весовой коэффициент $к_i$	Значение формантного параметра речи ΔA_i, дБ
1	125	53	0,01	25
2	250	66	0,03	18
3	500	66	0,12	14
4	1000	61	0,20	9
5	2000	56	0,30	6
6	4000	53	0,26	5
7	8000	49	0,07	4

Таблица 4

Результаты измерений при использовании лазерного доплеровского виброметра PDV-100 (видимый диапазон длин волн)

Тип пленки	№ полосы	Зеркальное отражение			Диффузное отражение (β = 200)		
		$L_{ии}$, дБ	$V_{ии}$,дБ	$V_{ши}$,дБ	$L_{ии}$,дБ	$V_{ии}$,дБ	$V_{ши}$,дБ
Silver 40	1	62,3	51,2	41,2	62,3	61,6	44,5
	2	63,1	48,6	34,3	63,1	56,7	40,4
	3	67,7	56,8	27,4	67,7	55,1	31,9
	4	68	64	32,3	68	50,6	37,9
	5	69,8	60,8	27,9	69,8	61,6	46,6
	6	72,5	55,2	28,8	72,5	71	55,6
	7	74,6	45,7	32,9	74,6	68,3	67,4
Silver 25	1	62,3	54,2	44,4	62,3	64,9	47,1
	2	63,1	48,3	35,8	63,1	59	39,2
	3	67,7	56,8	25,9	67,7	58,9	33,4
	4	68	64,3	30	68	52,1	35,9
	5	69,8	62,6	26,9	69,8	62,3	44,3
	6	72,5	56,6	28,8	72,5	70,8	53,3
	7	74,6	51,8	33,1	74,6	70,9	65,4

Продолжение таблицы 4

Тип пленки	№ полосы	Зеркальное отражение			Диффузное отражение (β = 200)		
		$L_{ии}$, дБ	$V_{ии}$,дБ	$V_{ши}$,дБ	$L_{ии}$,дБ	$V_{ии}$,дБ	$V_{ши}$,дБ
Silver 15	1	62,3	54,1	42,1	62,3	69,1	60,4
	2	63,1	48,3	33,8	63,1	64,4	63,3
	3	67,7	56,1	27,7	67,7	67,3	66,2
	4	68	63,6	31	68	70,2	69,1
	5	69,8	62,2	28,6	69,8	73,8	72
	6	72,5	54,4	30	72,5	76,7	75,2
	7	74,6	48,5	35,5	74,6	80,2	79,2
Silver 5	1	62,3	52	39,7	62,3	84,4	84,7
	2	63,1	47,2	29,9	63,1	87,2	87,8
	3	67,7	56	25,7	67,7	90,2	90,7
	4	68	63,8	30,3	68	93,2	93,7
	5	69,8	61,4	28,1	69,8	96,2	96,7
	6	72,5	54,8	31,8	72,5	99,2	99,7
	7	74,6	50,1	41,8	74,6	102,2	102,7
Silver 25 + Silver 5	1	62,3	48,3	39	–	–	–
	2	63,1	45,3	37,2	–	–	–
	3	67,7	52,8	30,8	–	–	–
	4	68	63	32,9	–	–	–
	5	69,8	60,2	38,9	–	–	–
	6	72,5	54,9	47,7	–	–	–
	7	74,6	62,5	60	–	–	–
Silver 15 + Silver 5	1	62,3	47,3	37,6	–	–	–
	2	63,1	48,1	37,2	–	–	–
	3	67,7	53,7	35	–	–	–
	4	68	61,6	31,6	–	–	–
	5	69,8	58,9	35,9	–	–	–
	6	72,5	52,3	44,5	–	–	–
	7	74,6	57,1	56,7	–	–	–
Silver 5 + Silver 5	1	62,3	96,4	84,7	–	–	–
	2	63,1	87,2	87,8	–	–	–
	3	67,7	90,2	90,7	–	–	–
	4	68	93,2	93,7	–	–	–
	5	69,8	96,2	98,7	–	–	–
	6	72,5	97,2	99,7	–	–	–
	7	74,6	100,2	101,3	–	–	–

Таблица 5

Результаты измерений при использовании лазерного доплеровского виброметра RSV-150 (инфракрасный диапазон длин волн)

Тип пленки	№ полосы	Зеркальное отражение			Диффузное отражение (β = 400)		
		$L_{ии}$, дБ	$V_{ии}$, дБ	$V_{ши}$, дБ	$L_{ии}$, дБ	$V_{ии}$, дБ	$V_{ши}$, дБ
Silver 40	1	68,3	64,1	51,6	68,3	65,3	55,5
	2	65,7	61,2	46,4	65,7	58,4	49,6
	3	72,3	52,2	41	72,3	58,6	50
	4	72,9	57,2	45,3	72,9	62,6	58,7
	5	75	69,8	53,4	75	69,7	67,6
	6	74,6	73,2	61,7	74,6	78,7	76,8
	7	76,6	73,5	70,8	76,6	86,3	85,7

Продолжение таблицы 5

Тип пленки	№ полосы	Зеркальное отражение			Диффузное отражение (β = 400)		
		$L_{ии}$, дБ	$V_{ии}$, дБ	$V_{ши}$, дБ	$L_{ии}$, дБ	$V_{ии}$, дБ	$V_{ши}$, дБ
Silver 25	1	68,3	67	53,3	68,3	61,9	58,4
	2	65,7	52,8	43,5	65,7	58,4	52,5
	3	72,3	50,4	37,2	72,3	55	47,1
	4	72,9	50,1	41,3	72,9	57	55,2
	5	75	54,9	45,8	75	65,3	64,1
	6	74,6	63,5	52,6	74,6	74,1	73,1
	7	76,6	61,2	59,8	76,6	82,4	82,1
Silver 15	1	68,3	63,3	57,5	68,3	64	58,9
	2	65,7	54,2	44,7	65,7	57,1	54,5
	3	72,3	53,8	36,9	72,3	49,4	49,1
	4	72,9	49,8	42,4	72,9	56,6	55,3
	5	75	57,2	48,6	75	65,6	64,1
	6	74,6	65,8	56,7	74,6	74,6	72,5
	7	76,6	64,4	64,3	76,6	83,5	83,3
Silver 5	1	68,3	63,1	59,8	68,3	58,5	58,4
	2	65,7	53,1	47,1	65,7	53,5	53,4
	3	72,3	48,8	35,9	72,3	52,1	52
	4	72,9	51,2	41,3	72,9	58,7	58,5
	5	75	55,5	45,9	75	67,7	67,6
	6	74,6	57,4	52,6	74,6	76,8	76,5
	7	76,6	62,7	59,9	76,6	85,8	85,5
Silver 25 + Silver 5	1	66,1	64,3	63,4	–	–	–
	2	66,7	57,2	56,8	–	–	–
	3	66,4	50,7	50,2	–	–	–
	4	69,1	59,4	59,2	–	–	–
	5	70,5	68,3	68	–	–	–
	6	71,1	77,3	77	–	–	–
	7	73,2	86,3	85,9	–	–	–
Silver 15 + Silver 5	1	66,1	65,2	64,6	–	–	–
	2	66,7	61,6	60,7	–	–	–
	3	66,4	54	53,8	–	–	–
	4	69,1	54,8	54,5	–	–	–
	5	70,5	63,5	63,1	–	–	–
	6	71,1	72,4	72,3	–	–	–
	7	73,2	81,5	81,4	–	–	–
Silver 5 + Silver 5	1	66,1	62,1	62	–	–	–
	2	66,7	55,7	55,6	–	–	–
	3	66,4	51,5	51,3	–	–	–
	4	69,1	60	59,9	–	–	–
	5	70,5	69	68,9	–	–	–
	6	71,1	78,8	77,9	–	–	–
	7	73,2	87,9	86,9	–	–	–

Таблица 6

Расчетные значения разборчивости речи при использовании лазерного доплеровского виброметра PDV-100 (видимый диапазон длин волн)

Тип пленки	Коэффициент светопропускания в видимом диапазоне, %	Разборчивость речи W, %	
		Зеркальное отражение	Диффузное отражение ($\beta = 20^0$)
Silver 40	47	99,7	98,4
Silver 25	29	99,7	99
Silver 15	21	99,6	44
Silver 5	7	99,6	0
Silver 25 + Silver 5	2	98,8	0
Silver 15 + Silver 5	1,3	98,9	0
Silver 5 + Silver 5	0,5	0	0

Таблица 7

Расчетные значения разборчивости речи при использовании лазерного доплеровского виброметра RSV-150 (инфракрасный диапазон длин волн)

Тип пленки	Коэффициент светопропускания в инфракрасном диапазоне, %	Разборчивость речи W, %	
		Зеркальное отражение	Диффузное отражение ($\beta = 40^0$)
Silver 40	31	94,6	56,0
Silver 25	28	89,5	41,2
Silver 15	20	88,6	28,2
Silver 5	7	86,7	1,77
Silver 25 + Silver 5	2	12,5	–
Silver 15 + Silver 5	1,4	11,2	–
Silver 5 + Silver 5	0,5	8,84	–

излучения от жалюзи наблюдается резкий «срыв» разборчивости речи при светопропускании пленки менее 1,5 – 2%;

б) при диффузном отражении от жалюзи разборчивость речи наблюдается резкий «срыв» разборчивости речи при светопропускании пленки менее 20%;

в) очевидно, что «срыв» разборчивости речи наблюдается, когда уровень отраженного от ламели сигнала становится ниже порога чувствительности приемника лазерного виброметра.

Учитывая, что «лазерные микрофоны» имеют мощность излучения от нескольких десятков до нескольких сотен мВт и более, можно сделать вывод о том, что использование светозащитных пленок в качестве средств защиты помещений от утечки речевой информации по акустооптическому каналу, если на окнах внутри защищаемого помещения установлены жалюзи, нецелесообразно, ввиду их низкой эффективности.

Литература

1. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008 – 436 с.

2. Лысов А.В. Оптические системы зондирования акустически возбужденных поверхностей (Лазерные системы акустической разведки). – СПб.: Медиапапир, 2020. – 512 с.

3. Солнцезащитные пленки [Электронный ресурс]. –– URL: https://www.solarblock.ru/ (дата обращения: 14.05.2021).

4. Gergely Takács1 , Jakub Otčenáš2 , Ján Vachálek3 , Boris Rohal'-Ilkiv4. Modal response-based technical countersurveillance measure against laser microphones // Journal of Vibroengineering. – Vol. 18, Issue 5, 2016, p. 3369-3382.

5. Sen Taner. Reflection Properties of a Gaussian Laser Beam from Multilayer Dielectric Films // Master's

Thesis. Izmir Institute of Technology, Urla Izmir, Turkey 2009. [Электронный ресурс]. – URL: https://core.ac.uk/download/pdf/324140029.pdf (дата обращения: 14.05.2021).

6. Золотарева К.Н. Организационные методы противодействия лазерным микрофонам. [Электронный ресурс]. – URL: http://www.spoisu.ru/files/riib/riib_1_2015.pdf (дата обращения: 14.05.2021).

References

1. Khorev A.A. Tekhnicheskaya zashchita informatsii: ucheb. posobiye dlya studentov vuzov. V 3-kh t. T. 1. Tekhnicheskiye kanaly utechki informatsii. - M.: NPTS «Analitika», 2008 – 436 s.–1.

2. Lysov A.V. Opticheskiye sistemy zondirovaniya akusticheski vozbuzhdennykh poverkhnostey (Lazernyye sistemy akusticheskoy razvedki). – SPb.: Mediapapir, 2020. – 512 s.

3. Solntsezashchitnyye plenki [Elektronnyy resurs]. –– URL: https://www.solarblock.ru/ (data obrashcheniya: 14.05.2021).–1.

Gergely Takács1 , Jakub Otčenáš2 , Ján Vachálek3 , Boris Rohal'-Ilkiv4. Modal response-based technical countersurveillance measure against laser microphones // Journal of Vibroengineering. – Vol. 18, Issue 5, 2016, p. 3369-3382.

Sen Taner. Reflection Properties of a Gaussian Laser Beam from Multilayer Dielectric Films // Master's Thesis. Izmir Institute of Technology, Urla Izmir, Turkey 2009. [Электронный ресурс]. – URL: https://core.ac.uk/download/pdf/324140029.pdf (дата обращения: 14.05.2021).

6. Zolotareva K.N. Organizatsionnyye metody protivodeystviya lazernym mikrofonam. [Elektronnyy resurs]. – URL: http://www.spoisu.ru/files/riib/riib_1_2015.pdf (data obrashcheniya: 14.05.2021).

ХОРЕВ Анатолий Анатольевич, доктор технических наук, профессор, заведующий кафедрой «Информационная безопасность», Национальный исследовательский университет «МИЭТ». 124498, г. Москва, г. Зеленоград, площадь Шокина, дом 1. Email: horev@miee.ru

СУРОВЕНКОВ Дмитрий Борисович, аспирант кафедры «Информационная безопасность», Национальный исследовательский университет «МИЭТ». 124498, г. Москва, г. Зеленоград, площадь Шокина, дом 1. Email: dimasurovenkov@yandex.ru

САВИН Андрей Дмитриевич, студент кафедры «Информационная безопасность», Национальный исследовательский университет «МИЭТ». 124498, г. Москва, г. Зеленоград, площадь Шокина, дом 1. Email: ondreysavin@gmail.com

HOREV Anatoly, Doctor of Technical Sciences, Professor, Head of the Department «Information security», National Research University of Electronic Technology (MIET), Id. 1, Shokin Square, Zelenograd, Moscow, Russia, 124498. Email: horev@miee.ru

SUROVENKOV Dmitry, PhD student of the Department «Information Security», National Research University of Electronic Technology (MIET), Id. 1, Shokin Square, Zelenograd, Moscow, Russia, 124498. Email: dimasurovenkov@yandex.ru

SAVIN Andrey, student of the Department «Information Security», National Research University of Electronic Technology (MIET), Id. 1, Shokin Square, Zelenograd, Moscow, Russia, 124498. Email: ondreysavin@gmail.com

УДК 004.056.57

Вестник УрФО № 2(40) / 2021, с. 14–21

Князева Н.С.

DOI: 10.14529/secur210202

ВОССТАНОВЛЕНИЕ ПОСЛЕДОВАТЕЛЬНОСТИ ФАЙЛОВЫХ ОПЕРАЦИЙ С ПРИМЕНЕНИЕМ ТЕОРИИ ГРАФОВ ПРИ ПРОВЕДЕНИИ КОМПЬЮТЕРНЫХ ИССЛЕДОВАНИЙ

В статье представлен способ решения задачи по восстановлению последовательности операций, производимых над файлом, в ОС Windows с применением теории графов. Процесс изменения временных отметок представлен в виде ориентированного графа, в котором вершинами являются состояния временных отметок исследуемого файла, а ребрами — операции, производимые над ним. Для восстановления последовательности файловых операций необходимо определить все возможные маршруты между вершинами, соответствующими возможному начальному и имеющемуся конечному состояниям временных отметок. В работе рассмотрены и описаны алгоритмы поиска маршрутов в глубину и ширину. Сделан вывод о предпочтительности поиска в глубину. Результаты его применения продемонстрированы на не-скольких примерах.

Ключевые слова: *временные отметки, файловые операции, компьютерная криминалистика, орграф перехода, поиск в ширину, поиск в глубину.*

RECOVERY THE SEQUENCE OF FILE OPERATIONS USING GRAPH THEORY IN COMPUTER FORENSICS INVESTIGATIONS

The paper presents a method for solving the problem of recovery the sequence of file operations in the Windows operating system using graph theory. The process of changing timestamps is represented as a directed graph, in which the vertices are the states of the timestamps of the file, and the edges are the file operations that were performed on the file. To restore the sequence of file operations, you need to determine all possible routes between the vertices. The paper considers and describes algorithms for searching routes in depth and width. The conclusion is made about the preference of the search in depth. The results of its application are demonstrated in several examples.

Keywords: *timestamps, file operations, computer forensics, transition digraph, breadth-first search, depth-first search.*

Опыт проведения компьютерных исследований и экспертиз показывает, что в процессе их выполнения эксперту-криминалисту приходится решать задачи, связанные с восстановлением последовательности файловых операций (ФОп), совершенных пользователем ПЭВМ в отношении интересуемых файлов, путем исследования метаданных файловой системы, в том числе временных отметок (ВО) файлов.

Анализ результатов цикла экспериментов [1, 2], проведенных в операционной системе (ОС) Windows, позволяет утверждать, что при совершении действий над файлами ВО изменяются по фиксированным алгоритмам, запрограммированным в ядре ОС.

С целью сопоставления возможных последовательностей ФОп наблюдаемым вариантам конечных состояний ВО файлов разработана модель изменения значений ВО [3], основанная на математическом аппарате теории автоматов. Модель наглядно демонстрирует, к каким состояниям ВО могут привести различные варианты последовательностей ФОп. На рис. 1 изображен пример моделирования процесса изменения ВО, осуществляемый при помощи таблицы переходов между состояниями ВО, где x_i — ФОп, s_j — состояния ВО. На рис. 1 представлен фрагмент таблицы переходов. Полная таблица построена на основе всего множества выявленных закономерностей изменения ВО [1, 2] и содержит 458 состояний [3]. Также в [3] приведена таблица соответствия x_i названиям ФОп.

В примере последовательное выполнение ФОп $x_6 \longrightarrow x_8 \longrightarrow x_{10}$ над файлом с изначальным состоянием ВО s0 привело к конечному состоянию ВО s_{50}:

$s_0 (x_6) \longrightarrow s_6$, $s_6 (x_8) \longrightarrow s_8$, $s_8 (x_{10}) \longrightarrow s_{50}$.

Под начальным состоянием будем считать состояние ВО файла s_0, который был создан и над которым файловые операции еще не совершались.

В ходе проведения криминалистических исследований эксперт может получить только конечные состояния ВО файлов. Поэтому методика восстановления ФОп заключается в определении конечного состояния (известного эксперту), а затем поиске ФОп и состояний, которые могли привести к имеющемуся конечному состоянию ВО по таблице переходов (рис. 2). При этом некоторые состояния могут быть обнаружены в таблице переходов на пересечении нескольких ФОп и состояний ВО, что приведет к появлению различных вариантов последовательностей ФОп.

Задачу поиска промежуточных состояний можно решить, используя теорию графов в два этапа. Для этого на первом этапе по таблице переходов необходимо построить

x(t)	S(t)															
	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}	s_{12}	s_{13}	…	s_{457}
x_1	s_1	s_1	s_{19}	s_1	s_1	s_1	s_{19}	s_{19}	s_{19}	s_1	s_{19}	s_{19}	s_{19}	s_{19}	…	s_{19}
x_2	s_2	s_2	s_2	s_2	s_2	s_2	s_2	s_2	s_2	s_2	s_2	s_2	s_2	s_2	…	s_2
x_3	s_3	s_3	s_3	s_3	s_3	s_{34}	s_3	s_{40}	s_{40}	s_3	s_3	s_{53}	s_{57}	s_{40}	…	s_{348}
x_4	s_4	s_4	s_4	s_{22}	s_4	s_{35}	s_4	s_{41}	s_{49}	s_{22}	s_{22}	s_{54}	s_{58}	s_{41}	…	s_{431}
x_5	s_5	s_5	s_5	s_5	s_5	s_5	s_5	s_{42}	s_{42}	s_5	s_5	s_5	s_5	s_{42}	…	s_5
x_6	s_6	s_{12}	s_{20}	s_{23}	s_{30}	s_{23}	s_{38}	s_{43}	s_{38}	s_{51}	s_{43}	s_{38}	s_{59}	s_{62}	…	s_{211}
x_7	s_7	s_{13}	s_{13}	s_{24}	s_{24}	s_{24}	s_7	s_7	s_7	s_7	s_7	s_7	s_{13}	s_{13}	…	s_{24}
x_8	s_8	s_{14}	s_{14}	s_{25}	s_{31}	s_{25}	s_8	s_{44}	s_8	s_{44}	s_{44}	s_8	s_{14}	s_{63}	…	s_{90}
x_9	s_9	s_{15}	s_{21}	s_{26}	s_{26}	s_{36}	s_{39}	s_{45}	s_{45}	s_9	s_{39}	s_{55}	s_{60}	s_{64}	…	s_{457}
x_{10}	s_6	s_{16}	s_{16}	s_{27}	s_{32}	s_{23}	s_6	s_{46}	s_{50}	s_{52}	s_{52}	s_{38}	s_{12}	s_{65}	…	s_{456}
x_{11}	s_{10}	s_{17}	s_{17}	s_{28}	s_{28}	s_{37}	s_{10}	s_{47}	s_{47}	s_{10}	s_{10}	s_{56}	s_{61}	s_{66}	…	s_{434}
x_{12}	s_{11}	s_{18}	s_{18}	s_{29}	s_{33}	s_{29}	s_{11}	s_{48}	s_{11}	s_{48}	s_{48}	s_{11}	s_{18}	s_{67}	…	s_{94}

Рис. 1. Моделирование процесса изменения ВО при выполнении последовательности ФОп $x_6 \longrightarrow x_8 \longrightarrow x_{10}$

x(t)	S(t)															
	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}	s_{12}	s_{13}	…	s_{457}
x_1	s_1	s_1	s_{19}	s_1	s_1	s_1	s_{19}	s_{19}	s_{19}	s_1	s_{19}	s_{19}	s_{19}	s_{19}	…	s_{19}
x_2	s_2	s_2	s_2	s_2	s_2	s_2	s_2	s_2	s_2	s_2	s_2	s_2	s_2	s_2	…	s_2
x_3	s_3	s_3	s_3	s_3	s_3	s_{34}	s_3	s_{40}	s_{40}	s_3	s_3	s_{53}	s_{57}	s_{40}	…	s_{348}
x_4	s_4	s_4	s_4	s_{22}	s_4	s_{35}	s_4	s_{41}	s_{49}	s_{22}	s_{22}	s_{54}	s_{58}	s_{41}	…	s_{431}
x_5	s_5	s_5	s_5	s_5	s_5	s_5	s_5	s_{42}	s_{42}	s_5	s_5	s_5	s_5	s_{42}	…	s_5
x_6	s_6	s_{12}	s_{20}	s_{23}	s_{30}	s_{23}	s_{38}	s_{43}	s_{38}	s_{51}	s_{43}	s_{38}	s_{59}	s_{62}	…	s_{211}
x_7	s_7	s_{13}	s_{13}	s_{24}	s_{24}	s_{24}	s_7	s_7	s_7	s_7	s_7	s_7	s_{13}	s_{13}	…	s_{24}
x_8	s_8	s_{14}	s_{14}	s_{25}	s_{31}	s_{25}	s_8	s_{44}	s_8	s_{44}	s_{44}	s_8	s_{14}	s_{63}	…	s_{90}
x_9	s_9	s_{15}	s_{21}	s_{26}	s_{26}	s_{36}	s_{39}	s_{45}	s_{45}	s_9	s_{39}	s_{55}	s_{60}	s_{64}	…	s_{457}
x_{10}	s_6	s_{16}	s_{16}	s_{27}	s_{32}	s_{23}	s_6	s_{46}	s_{50}	s_{52}	s_{52}	s_{38}	s_{12}	s_{65}	…	s_{456}
x_{11}	s_{10}	s_{17}	s_{17}	s_{28}	s_{28}	s_{37}	s_{10}	s_{47}	s_{47}	s_{10}	s_{10}	s_{56}	s_{61}	s_{66}	…	s_{434}
x_{12}	s_{11}	s_{18}	s_{18}	s_{29}	s_{33}	s_{29}	s_{11}	s_{48}	s_{11}	s_{48}	s_{48}	s_{11}	s_{18}	s_{67}	…	s_{94}

Рис. 2. Определение ФОп и состояния ВО, на пересечении которых находится конечное состояние ВО s_{50}

граф переходов [4], где вершины — состояния si, а ребра — операции x_j, производимые над файлом, петли свидетельствуют об операциях, возможно, производившихся над файлом неопределенное количество раз. На втором этапе в построенном орграфе переходов произвести полный перебор всех возможных маршрутов между конечной вершиной s_i, представляющей конечное состояние ВО, и начальной вершиной s_0, соответствующей начальному состоянию ВО.

Построенный на первом этапе граф является однонаправленным (орграф) и наглядно представляет переходы между состояниями s_i. Так, переходу к состоянию s_{50}, представленному на рис. 1, в графическом виде соответствует орграф, приведенный на рис. 3.

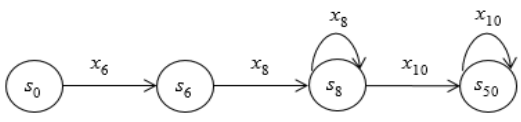

Рис. 3. Орграф перехода из состояния s_0 в состояние s_{50}

Исчерпывающий орграф переходов (рис. 4) построен по полной таблице переходов в программной среде MATLAB с применением функции digraph [5]. В качестве входных аргументов функции использовалась матрица смежности, сгенерированная на основе таблицы переходов. Сформированный таким образом орграф имеет 458 вершин и 3654 ребра.

Рис. 4. Орграф переходов, построенный по полной таблице переходов

На втором этапе для полного перебора всех возможных маршрутов между вершинами можно применять широко распространенные алгоритмы обхода графов: поиск

в ширину и глубину. Обход графа — это переход от одной его вершины к другой в поисках связей этих вершин, где в качестве связей имеются в виду ребра графа. В процессе обхода вершины могут находиться в трех состояниях: непросмотренные, просмотренные, использованные. Изначально все вершины имеют статус непросмотренных.

Алгоритм поиска в ширину (breadth-first search, BFS) подразумевает поуровневое исследование графа. Для описания поиска в ширину вводится очередь Q для хранения вершин. Поиск начинается с некоторой начальной вершины u. Эта вершина помещается в очередь Q и с этого момента считается *просмотренной*. Смежные с u вершины u_1, u_2, …, u_p, помещаются в очередь и получают статус *просмотренных*, а вершина u удаляется из очереди и получает статус *использованной*. Далее смежные с u_1, u_2, …, u_p вершины помещаются в очередь и получают статус *просмотренных*, а вершины u_1, u_2, …, u_p удаляются из очереди и получают статус *использованных*. Вершины просматриваются в порядке возрастания их расстояния от начальной вершины. В тот момент, когда очередь Q окажется пустой, поиск в ширину обойдет все вершины графа [6].

При поиске в глубину (depth-first search, DFS) производится перечисление вершин «вглубь», пока это возможно. Поиск начинается с некоторой начальной вершины u и с этого момента, она считается *просмотренной*. Если среди вершин, смежных с u, существует еще непросмотренная вершина w, тогда w объявляется *просмотренной*, и поиск продолжается из этой вершины. Если все вершины, смежные с u, просмотрены, тогда u объявляется *использованной* вершиной. Если в графе не осталось непросмотренных вершин, то поиск заканчивается. Если же осталась непросмотренная вершина, то поиск продолжается из нее [6].

На рис. 5 представлен процесс обхода орграфа алгоритмами поиска в ширину (а) и в глубину (б) из вершины s_{50}. Данные алгоритмы были реализованы в MATLAB с помощью функций bfsearch [7] и dfsearch [8] соответственно.

На рис. 5 сплошной линией выделены ребра, которые ведут к непросмотренным вершинам; штрихпунктирной линией — ребра, которые ведут к просмотренным вершинам; штриховой линией — ребра, которые ведут к использованным вершинам. Пошаговый процесс обхода в ширину и глубину графа представлен в таблицах 1 и 2 соответственно.

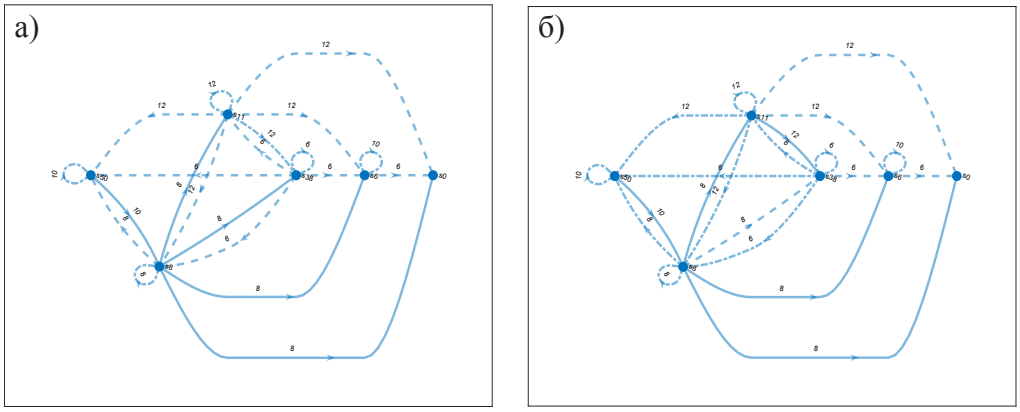

Рис. 5. Процесс обхода орграфа алгоритмами поиска в ширину и в глубину

Оба алгоритма приводят к идентичному результату, имеют одинаковую трудоемкость и позволяют обнаруживать все маршруты, соединяющие две вершины: начальную и конечную. При этом поиск в ширину зачастую используется для нахождения кратчайшего маршрута между точками. Поиск в глубину применяется для определения любого возможного маршрута между двумя вершинами и обнаружения циклов на графе.

Следует обратить внимание, что специфика орграфа переходов между состояниями ВО такова, что оба алгоритма приводят к появлению циклов. С точки зрения восстановления последовательности ФОп циклы и петли интерпретируются как повторение некоторых ФОп неопределенное количество раз. С одной стороны для полноты картины эту информацию надо учитывать. С другой стороны, в ходе компьютерного исследования следствие интересует в первую очередь по-

Таблица 1

Пошаговый процесс обхода в ширину

№ шага	Вершины, находящиеся в очереди Q	Статус вершины	Смежные вершины	Статус смежной вершины	Ребро, соединяющее вершины из очереди и смежную	Тип линии на рис. 5, а
1	s50	просмотренная				
2	s50		s8	непросмотренная	s50s8	сплошная
3	s50	использованная				
4	s8	просмотренная				
5			s0	непросмотренная	s8s0	сплошная
6			s6	непросмотренная	s8s6	сплошная
7			s11	непросмотренная	s8s11	сплошная
8			s38	непросмотренная	s8s38	сплошная
9			s50	использованная	s8s50	штриховая
10	s8	использованная				
11	s0	просмотренная				
12	s6	просмотренная				
13	s11	просмотренная				
14	s38	просмотренная				
15	s0		—			
16	s0	использованная				
17	s6		s0	использованная	s6s0	штриховая
18	s6	использованная				
19	s11		s0	использованная	s11s0	штриховая
20			s6	использованная	s11s6	штриховая
21			s8	использованная	s11s8	штриховая
22			s38	просмотренная	s11s38	штрихпунктирная
23			s50	использованная	s11s50	штриховая
24	s11	использованная				
25	s38		s6	использованная	s38s6	штриховая
26			s8	использованная	s38s8	штриховая
27			s11	использованная	s38s11	штриховая
28			s50	использованная	s38s50	штриховая
29	s38	использованная				

Таблица 2

Пошаговый процесс обхода в глубину

№ шага	Рассматриваемые вершины	Статус вершины	Смежные вершины	Статус смежной вершины	Ребро, соединяющее вершины из очереди и смежную	Тип линии на рис. 5, б
1	s50	просмотренная				
2	s50		s8	непросмотренная	s50s8	сплошная
3	s8	просмотренная				

Продолжение таблицы 2

№ шага	Рассматриваемые вершины	Статус вершины	Смежные вершины	Статус смежной вершины	Ребро, соединяющее вершины из очереди и смежную	Тип линии на рис. 5, б
4	s8		s0	непросмотренная	s8s0	сплошная
5	s0	просмотренная				
6	s0		—			
7	s0	использованная				
8	s8		s6	непросмотренная	s8s6	сплошная
9	s6	просмотренная				
10	s6		s0	использованная	s6s0	штриховая
11	s6	использованная				
12	s8		s11	непросмотренная	s8s11	сплошная
13	s11	просмотренная				
14	s11		s0	использованная	s11s0	штриховая
15			s6	использованная	s11s6	штриховая
16			s8	просмотренная	s11s8	штрихпунктирная
17			s38	непросмотренная	s11s38	сплошная
18	s38	просмотренная				
19	s38		s6	использованная	s38s6	штриховая
20			s8	просмотренная	s38s8	штрихпунктирная
21			s11	просмотренная	s38s11	штрихпунктирная
22			s50	просмотренная	s38s50	штрихпунктирная
23	s38	использованная				
24	s11		s50	просмотренная	s11s50	штрихпунктирная
25	s11	использованная				
26	s8		s38	использованная	s8s38	штриховая
27			s50	просмотренная	s8s50	штрихпунктирная
28	s8	использованная				
29	s50	использованная				

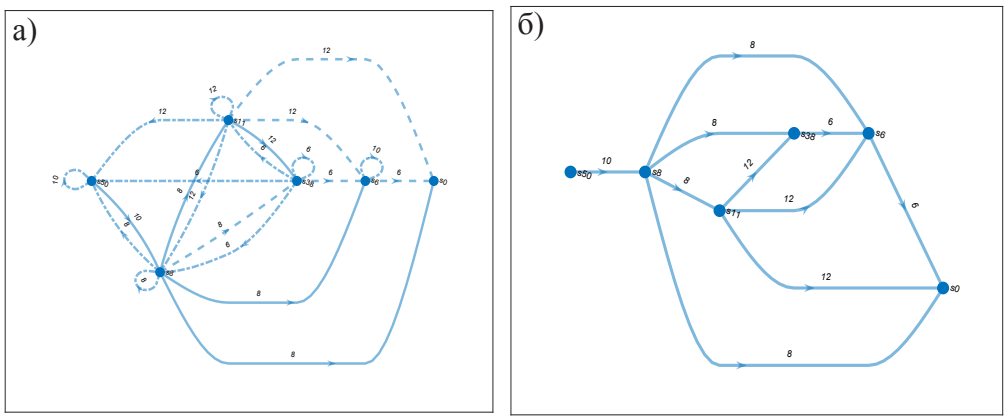

Рис. 6. Процесс обхода орграфа алгоритмом поиска в глубину с циклами и петлями (а) и без циклов и петель (б)

следовательность и факт выполнения ФОп, а не количество повторения однотипных операций. Поэтому, чтобы избежать избыточности информации циклы и петли из графа целесообразно исключать, что возможно при применении поиска в глубину. Для этого исключаются ребра, которые ведут к просмотренным вершинам (штрихпунктирная линия). На рис. 6, б изображен орграф процесса обхода в глубину без циклов и петель.

Орграф, построенный на рис. 6, б наглядно демонстрирует, какие ФОп могли быть совершены над исследуемым файлом. При этом последовательность ФОп восстанавливается от последней выполненной над файлом операции к первой. Между конечной и начальной вершинами могут быть обнаружены несколько маршрутов, что приведет к выявлению различных возможных вариантов последовательностей ФОп. Так, для примера, приведенного на рис. 6, б между вершинами, соответствующими состояниям ВО s50 и s0, возможны следующие варианты маршрутов:

$s_{50}(x_{10}) \longrightarrow s_8, s_8\,(x_8) \longrightarrow s_6, s_6\,(x_6) \longrightarrow s_0.$

$s_{50}(x_{10}) \longrightarrow s_8, s_8\,(x_8) \longrightarrow s_{38}, s_{38}\,(x_6) \longrightarrow s_6, s_6\,(x_6) \longrightarrow s_0.$

$s_{50}(x_{10}) \longrightarrow s_8, s_8\,(x_8) \longrightarrow s_{11}, s_{11}(x_{12}) \longrightarrow s_{38}, s_{38}\,(x_6) \longrightarrow s_6, s_6\,(x_6) \longrightarrow s_0.$

$s_{50}(x_{10}) \longrightarrow s_8, s_8\,(x_8) \longrightarrow s_{11}, s_{11}(x_{12}) \longrightarrow s_6, s_6\,(x_6) \longrightarrow s_0.$

$s_{50}(x_{10}) \longrightarrow s_8, s_8\,(x_8) \longrightarrow s_{11}, s_{11}(x_{12}) \longrightarrow s_0.$

$s_{50}(x_{10}) \longrightarrow s_8, s_8\,(x_8) \longrightarrow s_0.$ (1)

В (1) все варианты маршрутов начинаются с операций x_{10} и x_8. Таким образом, для состояния ВО s_{50} однозначно оказываются определены последняя ФОп (x_{10}) и предпоследняя ФОп (x_8).

Ниже представлены примеры процесса обхода орграфа из вершин, соответствующих состояниям ВО s_{32} и s_{71}.

Пример на рис. 7, а также демонстрируют однозначное определение последней и предпоследней ФОп, что очевидно следует из особенностей таблицы переходов: состояния ВО повторяются только по горизонтали для всех ФОп, за исключением x_6 (перемещение/переименование) и x_{10} (изменение атрибутов) [3].

Для уменьшения количества вариантов возможных маршрутов можно произвести их постобработку путем исключения некоторых ребер и вершин по имеющимся исходным условиям. Например, если известно, что все операции производились в ОС Windows 7, тогда можно исключить ребра, соответствующие ФОп, производимых в других версиях ОС Windows. В примере на рис. 7, б можно исключить все ребра, соответствующие ФОп x_{10}, в результате количество маршрутов уменьшится на 6.

Таким образом, решение задачи по восстановлению последовательности ФОп сводится к выполнению двух этапов, которые необходимо произвести один раз. Сначала следует сформировать орграф переходов по полной таблице переходов (рис. 4), который является универсальным для 12 ФОп в ОС Windows [1, 2]. Затем для всех вершин орграфа (состояний ВО) произвести поиск в глубину и исключить циклы и петли.

Данный процесс был запрограммирован в MATLAB. Для имеющейся таблицы переходов построение орграфа и расчет маршрутов для всех вершин заняло 8 минут на ПЭВМ «ПК Аквариус» (Intel(R) Core(TM) i5-4670 CPU @ 3,40GHz, 3,40 GHz, ОЗУ 16,00 ГБ). В результате была сформирована таблица, на вход которой эксперт может подавать конечное состояние ВО исследуемого файла s_i, а на выходе получать набор возможных вариантов после-

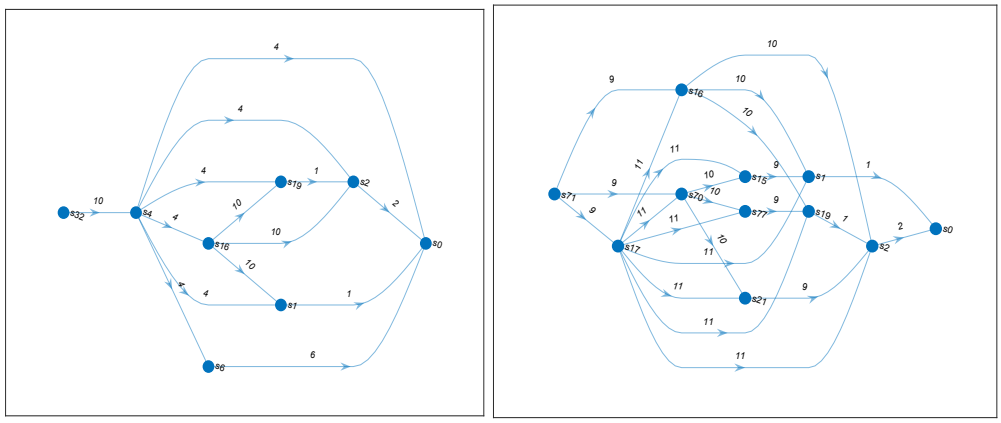

Рис. 7. Процесс обхода орграфа алгоритмом поиска в глубину из вершин, соответствующих состояниям ВО s_{32} (а) и s_{71} (б)

довательностей ФОп. Так как последовательности ФОп заранее посчитаны и помещены в таблицу, их формирование на выходе программы происходит практически мгновенно. Для эксперта этот процесс осуществляется «прозрачно». Ему остается только исключить явно невозможные ФОп по известным дополнительным условиям.

Литература

1. Духан Е.И., Князева Н.С. Методика и результаты исследования изменений временных отметок файловых объектов. // Радиотехника. 2020. Том 84, № 2 (4). С. 64-72.

2. Knyazeva N., Khorkov D., Vostretsova E. Building Knowledge Bases for Timestamp Changes Detection Mechanisms in MFT Windows OS. // Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). 2020. С. 553-556.

3. Knyazeva N., Duhan E. Timestamp Change Model in Windows OS. // Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). 2020. С. 623-626.

4. Советов Б.Я. Моделирование систем: Учебник для вузов / Б. Я. Советов, С. А. Яковлев. 5-е изд. М.: Высш. шк., 2007. 343 с.

5. Graph with directed edges – MATLAB [Электронный ресурс] // URL: https://ch.mathworks.com/help/matlab/ref/digraph.html (дата обращения: 01.04.2021).

6. Асанов М.О., Баранский В.А., Расин В.В. Дискретная математика: графы матроиды, алгоритмы // Ижевск: НИЦ «РХД». 2001. 288 с.

7. Breadth-first graph search – MATLAB bfsearch [Электронный ресурс] // URL: https://ch.mathworks.com/help/matlab/ref/graph.bfsearch.html (дата обращения: 01.04.2021).

8. Depth-first graph search – MATLAB dfsearch [Электронный ресурс] // URL: https://ch.mathworks.com/help/matlab/ref/graph.dfsearch.html (дата обращения: 01.04.2021).

References

1. Duhan E., Knyazeva N. Methodology and results of the study of changes in the timestamps of file objects [Metodika i rezul'taty issledovanija izmenenij vremennyh otmetok fajlovyh obektov]. // Radio engineering [Radiotehnika]. 2020. Vol. 84, no 2 (4). pp. 64-72.

2. Knyazeva N., Khorkov D., Vostretsova E. Building Knowledge Bases for Timestamp Changes Detection Mechanisms in MFT Windows OS. // Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). 2020. pp. 553-556.

3. Knyazeva N., Duhan E. Timestamp Change Model in Windows OS. // Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). 2020. pp. 623-626.

4. Sovetov B.Ya. Simulation of systems: Textbook for universities [Modelirovanie system: Uchebnik dlja vuzov] / B.Ya. Sovetov, S.A. Yakovlev 5-ye izd. M.: High school [Vysshaja shkola], 2007. 343 p.

5. Graph with directed edges – MATLAB. Available at: https://ch.mathworks.com/help/matlab/ref/digraph.html (accessed 01 April 2021).

6. Asanov M.O., Baranskij V.A., Rasin V.V. Discrete mathematics: graphs, matroids, algorithms [Diskretnaja matematika: grafy matroidy, algoritmy] // Izhevsk: NIC «RHD». 2001. 288 p.

7. Breadth-first graph search – MATLAB bfsearch. Available at: https://ch.mathworks.com/help/matlab/ref/graph.bfsearch.html (accessed 01 April 2021).

8. Depth-first graph search – MATLAB dfsearch. Available at: https://ch.mathworks.com/help/matlab/ref/graph.dfsearch.html (accessed 01 April 2021).

КНЯЗЕВА Наталия Сергеевна, старший преподаватель учебно-научного центра «Информационная безопасность», Уральский Федеральный Университет им. первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 32. E-mail: npalceva@inbox.ru.

KNYAZEVA Natalija, Senior lecturer of educational and scientific center «Information security», Ural Federal University named after the first President of Russia B.N.Yeltsin, 620002, Yekaterinburg, Mira str., 32. E-mail: npalceva@inbox.ru.

УДК 004.451.56 Вестник УрФО № 2(40) / 2021, с. 22–30

Окороков В. А., Лащук Д. Е.

DOI: 10.14529/secur210203

ПРИМЕНЕНИЕ СХЕМЫ МНОГОУРОВНЕВОГО ДОСТУПА ДЛЯ ОРГАНИЗАЦИИ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

Предотвращение утечек конфиденциальной информации, хранящейся и обрабатываемой вычислительными системами, является одной из важнейших проблем, с которыми приходится сталкиваться при обработке данных с ограниченным доступом, в частности персональных данных. К настоящему моменту существует множество примеров, когда конфиденциальные данные похищаются злоумышленниками и используются ими в преступных целях или оказываются доступными широкому кругу пользователей Internet. Данное обстоятельство показывает необходимость разработки надежных механизмов, обеспечивающих разграничение доступа к данным, что позволяет минимизировать ущерб, возникающий из-за компрометации конфиденциальной информации.

Базовые механизмы, обеспечивающие разграничения доступа, обычно встроены в ядро операционной системы (ОС) и требуют значительных усилий для их реализации и настройки в рамках конкретного экземпляра ОС. В статье рассматривается один из основных методов разграничения доступа, который используются в защищенных операционных системах, а именно метод многоуровневого доступа. Реализация метода требует достаточно больших усилий разработчиков и зачастую связана с необходимостью модификации существующего прикладного программного обеспечения. Отмечается актуальность данной тематики для изучения курса «Безопасность операционных систем» студентами, обучающимися на направлениях, связанных с обеспечением информационной безопасности и защиты информации в вычислительных системах.

В рамках статьи рассмотрены различные подходы к реализации многоуровневого доступа и отмечены основные проблемы его реализации [1]. Рассмотрено также влияние ограничений для субъектов, имеющих различные уровни доступа, на основе использования дополнительных критериев безопасности для каждого субъекта и модификации методов трансформации разрешённых потоков информации в системе.

Ключевые слова: *операционные системы, доступ к информации, многоуровневый доступ, методы мандатного доступа, информационная безопасность.*

APPLICATION OF A MULTI-LEVEL ACCESS SCHEME FOR PROTECTING CONFIDENTIAL DATA

Preventing leaks of confidential information stored and processed by computer systems is one of the most important problems that one has to face when processing data with limited access, in particular personal data. By now, there are many examples when confidential data is stolen by intruders and used by them for criminal purposes or becomes available to a wide range of Internet users. This circumstance shows the need to develop reliable mechanisms that ensure the delimitation of access to data, which makes it possible to minimize the damage arising from the compromise of confidential information.

The basic mechanisms that provide access control are usually built into the operating system (OS) kernel and require significant effort to implement and configure within a specific OS instance. The article discusses one of the main methods of access control, which are used in protected operating systems, namely the multilevel access method. The implementation of the method requires a fairly large effort of developers and is often associated with the need to modify the existing application software. The relevance of this topic for the study of the course "Security of operating systems" by students enrolled in areas related to ensuring information security and information protection in computing systems is noted.

Within the framework of the article various approaches to the implementation of multilevel access are considered and the basic problems of its implementation are noted [1]. The influence of restrictions for subjects with different levels of access is also considered, based on the use of additional security criteria for each subject and modification of methods for transforming allowed information flows in the system.

Keywords: *operating systems, access to information, multi-level access, mandatory access methods, information security.*

Введение

В настоящее время проблема разграничения доступа в защищенных операционных системах является одной из самых острых. В связи с тем, что вычислительные системы обычно рассчитаны на работу в многопользовательском режиме, необходимо корректно обеспечивать поддержку разграничения доступа пользователей к ресурсам, связанным с хранением и обработкой данных. Важно исключить возможность несанкционированного доступа к конфиденциальной информации со стороны пользователей, которые не имеют таких полномочий [1].

В системах защиты информации должны быть реализованы два простых, но очень важных правила:

- компактность;
- простота.

Система защиты не должна заметно снижать производительность вычислительных систем, а также затруднять деятельность пользователей. При реализации этих критериев следует обеспечить контроль доступа и защиту данных [1].

Важность проблемы разграничения доступа в защищенных операционных системах (ОС) требует повышенного внимания к изучению существующих методов в рамках курса «Безопасность операционных систем». В данной статье рассматриваются методические основы и базовый теоретический материал, обеспечивающий изучение методов мандатного разграничения доступа в рамках упомянутого курса.

Многоуровневый доступ

Механизм дискреционного управления доступом, который изначально использовался в ОС семейства Linux, позволяет пользователям, владельцам файлов, явным образом указать возможность доступа субъектов, т.е. процессов, запущенных различными пользователями системы, к объектам (сущностям), которые могут быть файлами, папками и другими компонентами вычислительной системы. Однако данный механизм не предназначен для регулирования передачей информации между субъектами и объектами, содержащими данные различных уровней конфиденциальности. Например, если данные, хранящиеся в объекте с высоким уровнем конфиденциальности прочитаны процессом, имеющим высокий уровень доступа, они могут быть записаны в любой другой, доступный этому процессу на запись объект, который может иметь низкий уровень конфиденциальности, а механизм дискреционного управления доступом не может этому воспрепятствовать. Таким образом, в рамках использования механизма дискреционного управления доступом возможность изменения степени конфиденциальности информации при ее передаче от одного объекта другому может являться причиной утечки конфиденциальных данных.

Для регулирования потоков конфиденциальной информации используется многоуровневая (мандатная) модель доступа, которая предполагает, что все субъекты системы разбиваются на конечное число групп, в соответствии с уровнем допуска к информации, а объекты (сущности) аналогичным образом группируются по признаку конфиденциальности. Число групп субъектов и объектов совпадают. Предполагается также, что группы могут быть линейно упорядочены по убыванию уровня допуска субъекта и степени секретности объекта.

Детализация доступа внутри одного уровня обычно реализуется на базе использования системы категорий сущностей, для которых доступ может выполняться. Например, в рамках информационной системы может храниться секретная информация о характеристиках танков и ракет. При этом один субъект должен быть допущен только к информации о танках, а другой к информации о ракетах.

В защищенных ОС поддержка схемы многоуровневого управления доступом выполняется путем связывания с субъектами и объектами вспомогательных структур данных, называемых метками безопасности [2].

• Для субъектов доступа в метке содержится информация относительно уровней допуска субъекта, а также перечень категорий, которые в рамках указанного интервала уровней допуска, разрешены для просмотра субъектом.

• Для объектов доступа в метке указывается уровень конфиденциальности (секретности) информации и категория содержащихся в объекте данных.

Системы многоуровневой защиты основаны на использовании двух базовых моделей: Белла-ЛаПадулы и Биба, которые регулируют потоки информации внутри системы [1].

Модель Белла-ЛаПадулы

Наибольшей эффективностью с точки зрения сохранения конфиденциальности информации обладает модель Белла-ЛаПадулы [2].

Модель Белла-ЛаПадулы использует следующие принципы организации потоков данных в системе:

• Процесс пользователя (субъект доступа) может записать данные в некоторый объект, только в том случае, если его уровень допуска будет меньше или равен уровню конфиденциальности объекта.

• Процесс пользователя (субъект доступа) может читать данные, находящиеся в объекте, только в том случае, когда его уровень допуска больше или равен уровня конфиденциальности (секретности) объекта.

Таким образом, предотвращается передача секретных документов на более низкие уровни допуска.

В рамках модели создаются благоприятные условия для утери и нарушения целостности данных, поскольку данные пользователей высших уровней секретности могут несанкционированно модифицироваться или уничтожаться пользователями низших уровней секретности [2].

Как показано на рисунке 1, в рамках модели Белла-Ла Падулы передача информации осуществляется от объектов с низким уровнем секретности к объектам с высоким уровнем секретности.

Например, субъект X с уровнем доступа «Совершенно секретно» может читать данные, хранящиеся в объекте с уровнем секретности «Секретно» или «Совершенно секретно», а записывать только в объекты с уровнем

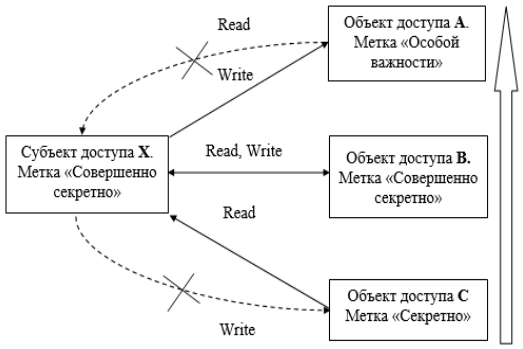

Рис. 1. Потоки данных в модели Белла-ЛаПадулы

секретности«Совершенно секретно» или «Особой важности».

Модель Биба

Модель Биба многоуровневого управления доступом характеризуется следующими базовыми свойствами [2]:

• Процесс пользователя (субъект доступа) может прочитать данные из некоторого объекта, только в том случае, если его уровень допуска будет меньше или равен уровню конфиденциальности объекта.

• Процесс пользователя (субъект доступа) может записывать данные, в некоторый объект, только в том случае, когда его уровень допуска больше или равен уровня конфиденциальности (секретности) объекта.

Таким образом, предотвращается модификация или уничтожение документов более высоких уровней конфиденциальности.

Следует отметить, что рассмотренные модели многоуровневой защиты несовместимы, т.к. позволяют обеспечить либо конфиденциальность, либо целостность данных.

Недостатки рассмотренных моделей можно частично устранить, если использовать вместо операции записи операцию добавления add. При добавлении данных потерь информации не происходит, что позволяет обеспечить целостность данных [4].

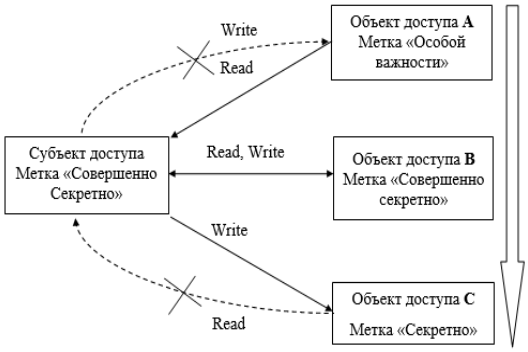

Рис. 2. Потоки данных в модели Биба

Как видно на рисунке 2, в рамках модели Биба передача информации осуществляется от объектов с высоким уровнем секретности к объектам с низким уровнем секретности. Такое направление потока данных в значительной степени гарантирует сохранение целостности информации, но при этом возможна утечка данных с высоким уровнем конфиденциальности (секретности).

Проблемы реализации мандатного управления доступом в защищенных ОС

В защищенных ОС механизм мандатного управления доступом является базовым механизмом разграничения доступа, однако при реализации и настройке этого механизма следует иметь в виду, что он не гарантирует полной защиты данных.

Существуют стандартные приемы взлома защиты, например, злоумышленник может найти в системе объект, в который возможна запись данных, и который не входит в область действия мандатного управления доступом. Такой объект может оказаться, например, в каталоге временных файлов /tmp.

Злоумышленник может также найти возможность для реализации передачи данных в оперативной памяти, например используя механизм разделяемой памяти, причем этот обмен не контролируется или некорректно контролируется механизмом защиты ОС. Часто такого рода обмен данными реализуются в программах, обеспечивающих графический интерфейс современных ОС. Возможен неконтролируемый обмен данными при использовании отладчиков, входящих в интегрированные среды программирования, а также при использовании процессами встроенных в ОС примитивов, обеспечивающих взаимодействие процессов.

На практике обычно не удается достигнуть абсолютной надежности системы мандатного управления доступом. Однако, можно либо значительно сократить возможности создания злоумышленником средств обмена данными, либо, либо сделать пропускную способность таких средств недостаточной для организации хищения конфиденциальных данных [3].

Одной из существенных проблем реализации мандатного доступа является возможность существования двунаправленных информационных потоков. Особенно часто с проблемой их реализации приходится сталкиваться при организации запросов к удаленному серверу, для которого обычно за-

прос на чтение данных и ответ пересылаются по одному каналу связи. В этом случае уровень конфиденциальности данных при передаче по сети может искажаться из-за различных уровней доступа процессов клиента и сервера. Например, если процесс с высоким уровнем доступа посылает запрос к данным, находящимся на сервере с низким уровнем доступа, то такой запрос не может быть обработан сервером из-за недостаточного уровня доступа. Если сервер имеет высокий уровень доступа, то все данные, которые он возвращает процессу будут также иметь высокий уровень конфиденциальности.

Довольно существенные проблемы возникают из-за возможной несовместимости мандатной модели с прикладным программным обеспечением. Например, для работы текстового редактора с документами, имеющими высокий уровень конфиденциальности, он должен иметь высокий уровень доступа. В тоже время при сохранении редактором документа с произвольным уровнем конфиденциальности, этому документу будет присваиваться уровень конфиденциальности, соответствующий уровню доступа редактора. Коррекция возможных ошибок в определении уровня конфиденциальности требует доработки прикладного программного обеспечения, что может привести к появлению запрещенных потоков данных.

К аналогичным проблемам может привести обращение субъектов с различными уровнями доступа к системным объектам или организации асинхронного доступа при реализации операций ввода-вывода.

Мандатное управление доступом в защищенных операционных системах

Основной задачей, решаемой путем реализации мандатного управления доступом в защищённых ОС, является уменьшение возможностей по созданию и эксплуатации средств, использующихся для хищения конфиденциальной информации, а также существенное снижение доступности их реализации злоумышленником. При этом даже при наличии уязвимостей в системе защиты снижается риск утечки конфиденциальных данных в результате ошибочных действий пользователя.

Злоумышленник, пытающийся преодолеть систему защиты, должен затратить значительные усилия на изучение системы и поиск уязвимостей. В результате вредоносное программное обеспечение, целью разработки которого является реализации хищения конфиденциальных данных, в условиях мандатного управления доступом оказывается практически бесполезным.

Сложные модели управления доступом в ОС семейства Linux иногда реализуются на базе использования пакета Security Enhanced Linux (SELinux). В современных защищенных ОС данный пакет обычно не используется, поскольку требует большой объем работ по проверке его корректности. Кроме того средства, которые используются для описания политики безопасности в рамках данного пакета, отличаются громоздкостью и их использование крайне неудобно. И главное, в пакет SELinux не включены утилиты, позволяющие обеспечивать контроль целостности информации в рамках многоуровневой модели доступа.

Одним из примеров успешной реализации мандатного доступа в защищенных ОС является операционная система специального назначения Astra Linux [5]. В рамках этой ОС реализация мандатного управления доступом базируется на использовании модуля подсистемы безопасности PARSEC, который совместно с подключаемыми модулями аутентификации PAM обеспечивает управление политикой безопасности ОС. Вместе с мандатным управлением доступом подсистема безопасности реализует мандатный контроль целостности и базовые функции аудита.

Для определения в некотором экземпляре ОС наименований мандатных уровней используется файл /etc/parsec/mac_levels, например:

Секретно:0

Совершенно секретно:1

Особой важности:2

Для определения именования неиерархических категорий используется файл /etc/parsec/mac_categories, например:

Танки:0

Ракеты:1.

Указанные файлы позволяют определить базовые атрибуты мандатной системы управления доступом.

При реализации иерархических категорий используется битовая маска, указывающая к каким категориям относится информация, хранящаяся в данном объекте. Количество бит в маске соответствует числу категорий, например для двух категорий из примера приведенного выше возможны следующие значения битовой маски:

00 - информация, хранящаяся в объекте, не имеет отношения ни к танкам, ни к ракетам;

01 - информация, хранящаяся в объекте, имеет отношения к танкам, но не к ракетам;

10 - информация, хранящаяся в объекте, имеет отношения к ракетам, но не к танкам;

11 - информация, хранящаяся в объекте, имеет отношение и к танкам, и к ракетам.

Значения параметров, которые были назначены субъектам доступа, и которые отображаются в соответствующих учетных записях, перечисляются в каталоге /etc/parsec/macdb. Структура каталога организована таким образом, что каждому пользователю, у которой указан отличный от нуля мандатный уровень или перечень неиерархических категорий, содержащий, по меньшей мере, одну категорию, создается отдельный текстовый файл, имя которого совпадает с идентификатором пользователя UID (User IDentifier). Файл содержит строку вида [5]:

<uname>:<umin_level>:<umin_categories>:<umax_level>:<umax_categories>

где:

uname - имя учётной записи пользователя;

umin_level - минимальный уровень допуска, доступный процессам, запущеным от имени учётной записи пользователя;

umin_categories – определяет минимальное множество неиерархических категорий, установленных для заданной учётной записи пользователя;

umax_level - максимальный уровень допуска, доступный процессам, запущеным от имени учётной записи пользователя;

umax_categories – определяет максимальное множество неиерархических категорий, доступных для некоторого пользователя.

Файл /etc/parsec/mac [5] содержит атрибуты суперпользователя root. Формат файла аналогичен формату файла обычного пользователя.

Метки, задающие конфиденциальность объектов, по умолчанию задаются следующим образом [5]:

1. Корневому каталогу присвоен наивысший уровень конфиденциальности, который может быть назначен в конкретной ОС (по умолчанию 3).

2. Предполагается возможность сохранения объектов, для которых заданы все возможные неиерархические категории.

3. Задаются атрибуты CCNR (определяет, что каталог может содержать сведения об объектах с различными метками безопасности, но не большими, чем его собственная метка) и CCNRI (определяет, что контейнер может содержать сведения об объектах с различными уровнями целостности, но не большими, чем его собственный уровень целостности).

Данный набор настроек фактически подразумевает, что в файловая система может сохранять любые данные с произвольными мандатными метками, при этом уровень конфиденциальности объектов не может превосходить некоторого максимально возможного значения, которое назначается корневому каталогу. Процесс с произвольным уровнем доступа, включая минимальный, может читать данные, находящиеся в каталоге, находящемся на вершине иерархии.

Стандартным директориям, например /bin, /etc, /lib, /usr и т.д., которые обеспечивают функционирование системы, назначается низший уровень конфиденциальности и пустая маска неиерархических категорий. В таком случае оказывается невозможным создание в перечисленных каталогах объектов с высоким уровнем конфиденциальности. Данное обстоятельство позволяет устранить значительную часть проблем, возникающих из-за возможной несовместимости системного и прикладного ПО с мандатным управлением доступом.

В параметрах каталога /dev, предназначенного для хранения системных файлов устройств, содержащих описания и параметры устройств, входящих в состав вычислительной системы, обычно назначается наивысший уровень конфиденциальности и устанавливается атрибут CCNR. Это позволяет создавать средствами ОС устройства, которые могут быть использованы для вывода конфиденциальных данных на внешние элементы вычислительной системы.

Основы администрирования мандатного управления доступом и контроль целостности в защищенных ОС

Возможности администрирования подсистемы, обеспечивающей мандатное управление доступом ОС Astra Linux, реализуются с помощью вспомогательной программы «Управление политикой безопасности», имеющей графический интерфейс. Данная программа может быть запущена с помощью пункта «Настройки» главного пользовательского

меню. В тоже время существует альтернативный способ управления уровнями доступа пользователей, который реализуется утилитой pdp-ulbls. При использовании этой утилиты возможно изменение уровней доступа субъектов и множества доступных им категорий. Наиболее часто использующийся набор параметров данной утилиты перечислен ниже:

pdp-ulbls -m<smin>:<smax> -c<cat-smin:cat-smax> <username>,

где:

smin - минимальный уровень доступа, задаваемый для пользователя;

smax - максимальный уровень доступа, задаваемый для пользователя;

cat-smin – определяет минимальный набор неиерархических категорий, задаваемый для учётной записи пользователя;

cat-smax - определяет максимальный набор неиерархических категорий, задаваемый для учётной записи пользователя.

<username> - имя пользователя.

Для решения задач контроля целостности в защищенных ОС реализованы следующие основные утилиты [5]:

• средство подсчета контрольных сумм файлов;

• средство контроля соответствия дистрибутиву;

• средства регламентного контроля целостности.

Утилита командной строки gostsum, входящая в набор утилит ОС, используется ля подсчета контрольных сумм файлов и оптических носителей.

Синтаксис утилиты командной строки х5ъ:

gostsum [КЛЮЧИ]... [ФАЙЛ]

Основные параметры утилиты [5]:

--gost-2012 - устанавливает, что будет использован алгоритм ГОСТ Р 34.11-2012 [6] с длиной хэш-кода 256 бит (по умолчанию);

--gost-2012-512 - устанавливает, что будет использован алгоритм ГОСТ Р 34.11-2012 с длиной хэш-кода 512 бит

-b - устанавливает размер блоков, которыми будет считываться файл

-o - задает имя файла для вывода контрольной суммы (по умолчанию - стандартный поток вывода);

-d - задает имя файла устройства чтения оптических дисков (файла с образом оптического диска) для подсчета контрольной суммы;

П р и м е р

Подсчет контрольной суммы оптического носителя

gostsum -d /dev/cdrom

Средство контроля соответствия дистрибутиву [5] предоставляет возможность контроля соответствия объектов файловой системы дистрибутиву ОС. Для обеспечения контроля целостности объектов в состав дистрибутива входит файл gostsums.txt со списком контрольных сумм по ГОСТ Р 34.11-2012 [6] с длиной хэш-кода 256 бит для всех файлов, входящих в пакеты программ дистрибутива.

Средства регламентного контроля целостности

Организация регламентного контроля целостности ОС, прикладного ПО и СЗИ обеспечивается набором программных средств на основе «Another File Integrity Checker» [5]. В указанном наборе реализована возможность для проведения периодического (с использованием системного планировщика заданий cron) вычисления контрольных сумм файлов и соответствующих им атрибутов расширенной подсистемы безопасности PARSEC (мандатных атрибутов и атрибутов расширенной подсистемы протоколирования) с последующим сравнением вычисленных значений с эталонными. В указанном наборе программных средств реализовано использование библиотеки libgost, обеспечивающей подсчет контрольных сумм в соответствии с ГОСТ Р 34.11-94 [6].

Эталонные значения контрольных сумм и атрибутов фалов хранятся в базе данных. База контрольных сумм и атрибутов может быть создана при помощи команды:

afick -i

Для вычисления контрольных сумм могут использоваться алгоритмы: MD5-Digest, SHA1 и ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит.

Заключение

В статье рассмотрен базовый теоретический материал, касающийся организации защиты информации в операционных системах семейства Linux. Отмечено, что использование традиционной для UNIX-подобных систем методики разграничения доступа к данным, основанной на дискреционной модели, не обеспечивает управления потоками информации в системе, что может стать причиной непреднамеренной утечки конфиденциальных сведений.

Показано, что наилучшим из существующих решений, реализованных в современных защищенных операционных системах, является применение методики мандатного доступа, базирующегося на реализации схемы многоуровневой системы защиты. Рассмотрены основные возможности защищенной ОС Astra Linux по организации поддержки многоуровневого доступа, а также сделан обзор существующих вспомогательных программ и структур данных, обеспечивающих реализацию и настройку многоуровневой модели доступа в рамках защищенной ОС.

Собранный в статье материал позволяет обеспечить изучение темы «Организация многоуровневой защиты в защищенных ОС» в рамках курса «Защита операционных систем», а также может быть использован для настройки многоуровневого доступа в экземплярах защищенных ОС.

Литература

1. Хартиков, Д. М. Исследование и разработка методов реализации мандатных средств управления доступом в сетевых ОС семейства UNIX: дис. … канд. тех. наук / Д. М. Хартиков – М.: МЦСТ, 2004. – 194 с.

2. Безбогов, А. А. Методы и средства защиты компьютерной информации: учеб. пособие / А. А. Безбогов, А. В. Яковлев, В. Н. Шамкин. – Тамбов: Изд-во ТГТУ, 2006. – 120 с.

3. Нестеров, С. А. Информационная безопасность и защита информации: учебное пособие. /С. А. Нестеров. СПб.: Изд-во политехн. ун-та, 2009. – 126 с.

4. Барабанов, А. В. Семь безопасных информационных технологий: мандатный метод управления доступом / А. В. Барабанов, А. В. Дорофеев, А. С. Марков, В. Л. Цирлов / под ред. <А. С. Маркова>. – М.: Изд-во ДМК ПРЕСС, 2017. – 224 с.

5. Операционная система специального назначения «Astra Linux special edition». Руководство по КСЗ. в 2 ч. Ч. 1: 2012. – 100 с.

6. ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования .- М.: Стандартинформ, 2013. -24 с.

References

1. Hartikov, D. M. Issledovanie i razrabotka metodov realizacii man-datnyh sredstv upravlenija dostupom v setevyh OC semejstva UNIX: dis. … kand. teh. nauk / D. M. Hartikov – M.: MCST, 2004. – 194 s.

2. Bezbogov, A. A. Metody i sredstva zashhity komp'juternoj informacii: ucheb. posobie / A. A. Bezbogov, A. V. Jakovlev, V. N. Shamkin. – Tambov: Izd-vo TGTU, 2006. – 120 s.

3. Nesterov, S. A. Informacionnaja bezopasnost' i zashhita informacii: uchebnoe posobie. /S. A. Nesterov. SPb.: Izd-vo politehn. un-ta, 2009. – 126 s.

4. Barabanov, A. V. Sem' bezopasnyh informacionnyh tehnologij: man-datnyj metod upravlenija dostupom / A. V. Barabanov, A. V. Dorofeev, A. S. Markov, V. L. Cirlov / pod red. <A. S. Markova>. – M.: Izd-vo DMK PRESS, 2017. – 224 s.

5. Operacionnaja sistema special'nogo naznachenija «Astra Linux special edition». Rukovodstvo po KSZ. v 2 ch. Ch. 1: 2012. – 100 s.

6. GOST R 34.11-2012 Informacionnaja tehnologija. Kriptograficheskaja zashhita informacii. Funkcija hjeshirovanija. – M.: Standartinform, 2013. – 24 s.

ОКОРОКОВ Валерий Анатольевич, кандидат физико-математических наук, доцент кафедры защиты информации ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект В.И. Ленина, д. 76. E-mail: okorokovva@susu.ru

ЛАЩУК Дмитрий Евгеньевич, студент кафедры защиты информации ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект В.И. Ленина, д. 76. E-mail: darthus7@mail.ru

OKOROKOV Valeriy, candidate of physical and mathematical sciences, Associate Professor of Department of Information Security Department of «South Ural State University». Russia, 454080, Ural Federal District, Chelyabinsk Region, Chelyabinsk, prosp. V. I. Lenin, 76. E-mail: okorokovva@susu.ru

LASHCHUK Dmitry, student of the Information Security Department of «South Ural State University». Russia, 454080, Ural Federal District, Chelyabinsk Region, Chelyabinsk, prosp. V. I. Lenin, 76. E-mail: darthus7@mail.ru

УДК 004.056.5: 004.822 Вестник УрФО № 2(40) / 2021, с. 31–43

Васильев В.И., Вульфин А.М., Кириллова А.Д., Никонов А.В.

DOI: 10.14529/secur210204

СИСТЕМА ОЦЕНКИ МЕТРИК ОПАСНОСТИ УЯЗВИМОСТЕЙ НА ОСНОВЕ ТЕХНОЛОГИЙ СЕМАНТИЧЕСКОГО АНАЛИЗА ДАННЫХ[1]

Предложена система прогнозирования компонент вектора метрик уязвимостей и количественной оценки степени опасности этих уязвимостей на основе анализа текстового описания с помощью инструментов обработки естественного языка (Natural Language Processing, NLP). Применение системы направлено на повышение оперативности оценки опасности выявляемых уязвимостей программно-аппаратного обеспечения автоматизированной системы управления технологическими процессами для соответствующего реагирования и принятия необходимых мер с целью обеспечения требуемого уровня кибербезопасности объектов и систем.

Ключевые слова: *информационная безопасность, угрозы, уязвимости, обработка естественного языка, CVSS, анализ текстов.*

Vasilyev V.I., Vulfin A.M., Kirillova A.D., Nikonov A.V.

SYSTEM FOR EVALUATING VULNERABILITY SEVERITY METRICS BASED ON SEMANTIC DATA ANALYSIS TECHNOLOGIES

A system for predicting the components of the vulnerability metrics vector and quantifying the severity of these vulnerabilities based on the analysis of the textual description using natural language processing (NLP) tools is proposed. The application of the system is aimed at increasing the efficiency of assessing the danger of the identified vulnerabilities of the software and hardware of the APCS for appropriate response and taking the necessary measures in order to ensure the required level of cybersecurity of objects and systems.

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-08-00668 и при финансовой поддержке Минобрнауки России (грант ИБ) № 1/2020.

Keywords: *information security, threats, vulnerabilities, natural language processing, CVSS, analysis of texts.*

Введение

Ежедневно регистрируются новые уязвимости программного и аппаратного обеспечения информационных систем (ИС), но их анализ и присвоение количественной оценки уровня опасности, по-прежнему, занимает продолжительное время (до трех месяцев). Согласно статистике компании Claroty [1], за 2020 год выявлено 893 уязвимостей, что на 24,72% больше, чем в 2019 году. Более 70% уязвимостей получили статус критических или высокую степень опасности.

В [2] на примере NVD (National Vulnerability Database – хранилище данных уязвимостей, основанное на стандартах правительства США) выполнен анализ зависимости времени появления эксплоита от компонент вектора метрик CVSS (Common Vulnerability Scoring System – общепринятый стандарт для определения степени опасности уязвимостей в программном обеспечении) уязвимостей. Показано, что существуют классы уязвимостей с очень коротким медианным временем появления эксплоитов (три дня). Отмечено, что временная задержка заполнения NIST (Национальный институт стандартов и технологий США) метрик CVSS после публикации уязвимости возросла с одного дня (для уязвимостей до 2017 года) до 19 дней (для уязвимостей, внесенных в базу в 2018 году). Напротив, среднее время появления эксплоита для уязвимостей сократилось с 296 дней в 2005 году до шести дней в 2018 году.

Важность наискорейшей оценки опасности уязвимости с момента ее регистрации в открытых источниках обусловлена высокой вероятностью ее эксплуатации злоумышленниками. Недостаток информации о степени опасности уязвимости и ее характеристиках осложняет планирование и проведение мероприятий по защите уязвимых ИС для специалистов. Следовательно, в ходе аудита ИС и инвентаризации программного обеспечения (ПО) важно иметь актуальную информацию по выявленным уязвимостям и количественным оценкам их опасности для эффективного планирования защитных мероприятий.

Целью работы является повышение эффективности (точности и оперативности) оценки опасности уязвимостей с помощью прогнозирования векторов метрики на основе анализа текстового описания.

1. Анализ применения технологий Text Mining в задаче оценки опасности уязвимостей

Исследованию возможностей методов семантического анализа текстов (Text Mining) для решения задач анализа и прогнозирования опасности уязвимостей ПО непосредственно по их текстовым описаниям, хранящимся в базах данных (БД) уязвимостей, посвящен ряд работ [3–12]. Так, в [3] авторы проанализировали появление новых записей CVE (база данных общеизвестных уязвимостей информационной безопасности) за 23 месяца и установили, что в среднем существует 132-дневный разрыв между объявлением уязвимости MITRE (некоммерческая организация, специализирующаяся в области системной инженерии) и моментом, когда NIST определяет уровень опасности уязвимости и метрики CVSS. Предложена система анализа уязвимостей, позволяющая прогнозировать эксплуатацию уязвимости и выполнять оценку компонент вектора метрик CVSS, используя текстовые данные обсуждения Twitter, собранные за три дня после даты первого упоминания уязвимости.

В [4] предложен новый подход к структурированию описаний уязвимостей, позволяющий в явном виде выделить условия реализации уязвимости как последовательность определенных событий – действий со стороны пользователей и атакующих, что важно в первую очередь для понимания характера уязвимости и способа ее устранения.

Авторы статьи [5] решают задачу оценки критичности (опасности) уязвимостей в два этапа, на первом из которых осуществляется векторизация (Word Embedding) текстовых описаний уязвимостей, а на втором производится классификация полученных векторов (наборов уникальных признаков описаний) с помощью методов машинного обучения.

В работе [6] используется аналогичный подход к оценке степени критичности уязвимостей, предполагающий на начальном этапе формирование словаря векторов слов для каждого описания уязвимости (для этого используется модель Skip-Gram алгоритма Word2Vec), а затем извлечение признаков текста на уровне предложений и классификация полученного вектора описаний уязвимости с помощью сверточной нейронной сети.

Статья [7] посвящена задаче ранжирования (приоритезации) уязвимостей ПО, для решения которой предложена следующая процедура: а) оформляется корпус CVE-описаний уязвимостей из базы данных NVD; б) производится конвертация CVE-описаний в «мешок слов» (модель CBOW); в) осуществляется ранжирование уязвимостей по степени важности с применением алгоритма TextRank, основанного на оценке семантической близости предложений в тексте.

В работе [8] использованы модели машинного обучения и обработки естественного языка для прогнозирования последствий кибератак. Представлена модель векторизации текстовых описаний новых кибератак и прогнозирования последствий для конечных пользователей. Создан набор данных о кибератаках с указанием их технических и нетехнических последствий. При помощи методов вложения слов (Doc2Vec) подготовлены данные для ансамбля моделей машинного обучения (LinearSVC, NB, MLP), оценка качества прогнозирования составила до 60 %.

В работе [9] предложена модель для прогнозирования компонент базового вектора CVSS с возможностью объяснения прогноза, которая использует текстовые описания новых уязвимостей. Применяются технологии Bag-of-Word и оценка энтропии вхождения слов в текстовые описания.

В работе [10] рассмотрен метод оценки CVSS на основе текстовых описаний уязвимостей из базы данных OSVDB. Выполнено извлечение и предобработка текстового описания уязвимостей, использованы методы LDA и PCA для уменьшения размеров вектора признаков, применены алгоритмы SVM и Random Forest, а также нечеткие системы для прогнозирования оценок компонент вектора CVSS. Лучший предиктор был получен с помощью нечеткой системы с точностью прогноза по шкале CVSS на уровне 88 %.

Анализ публикаций также показал, что прогнозирование оценки метрики CVSS опасностей уязвимостей выполнено для англоязычных описаний уязвимостей. Открытым остается вопрос о повышении оперативности оценки опасности уязвимостей для программных продуктов и систем, распространенных на локальных рынках, и для которых описания уязвимостей представлены, например, на русском языке. На примере Банка данных угроз безопасности информации (БДУ) ФСТЭК России рассмотрим возможность прогнозирования компонент вектора базовой метрики CVSS 2.0/3.0 и оценки уровня опасности уязвимостей на основе технологий Text Mining.

2. Архитектура системы оценки опасности уязвимостей на основе технологий интеллектуального анализа данных

Компоненты базовой метрики CVSS 2.0/3.0 представлены в таблице 1.

Оценка опасности уязвимости на основе базовой метрики (CVSS 2.0) определяется как:

$$BaseScore = (0{,}6 \cdot Impact + 0{,}4 \cdot Exploitability - 1{,}5) \cdot f(Impact), \quad (1)$$

где оценка воздействия:

$$Impact = 10{,}41 \cdot (1 - (1 - C) \cdot (1 - I) \cdot (1 - A)), \quad (2)$$

оценка возможности эксплуатации:

$$Exploitability = 20 \cdot AC \cdot Au \cdot AV, \quad (3)$$

$f(Impact) = 0$, если $Impact = 0$;

$f(Impact) = 1{,}176$ в других случаях.

Следовательно, возможно два подхода для оценки BaseScore CVSS 2.0/3.0:

– построение ансамбля предикторов для оценки отдельных значений компонент вектора (AV, AC, Au, C, I, A) по формализованному текстовому описанию с последующим расчетом по (1)–(3) результирующего значения;

– построение модели регрессии для непосредственной оценки результирующего значения по формализованному текстовому описанию.

Архитектура предлагаемой системы для прогнозирования оценки опасности уязвимости CVSS 2.0/3.0 представлена на рис. 1.

Первый этап работы системы связан со сбором и агрегацией специализированных новостных рассылок и тематических ресурсов в виде слабоструктурированных текстовых данных для построения документоориентированной БД$_1$ (MongoDB) с привязкой записей к ключу CVE-ID из БДУ ФСТЭК и NVD (CVE, CWE (БД недостатков ПО, которые могут быть использованы злоумышленниками), CPE (формальный язык описания всех возможных продуктов, операционных систем и аппаратных устройств при описании уязвимостей)). Процесс сбора данных регулируется специалистами по информационной безопасности с применением Threat Intelligence.

Затем собранные текстовые данные подвергаются предобработке и нормализации: символьная фильтрация, токенизация, фильтрация на основе стоп-словарей, лемматизация – на основе технологии конвейеризации NLP-Pipe.

Далее строится ансамбль Text Mining мо-

Таблица 1

Компоненты базовой метрики CVSS 2.0/3.0

Метрика	Буквенное обозначение	Возможные значения
Способ получения доступа (Access Vector – v2) (Attack Vector – v3)	AV	Physical (v3.0)
		Local (v2.0, 3.0)
		Adjacent (v2.0, 3.0)
		Network (v2.0, 3.0)
Сложность эксплуатации уязвимости (Access Complexity – v2) (Attack Complexity – v3)	AC	Lower (v2.0, 3.0)
		High (v2.0, 3.0)
		Medium (v2.0)
Показатель аутентификации (Authentication – v2) (Privileges Required – v3)	Au (v2.0) Pr(v3.0)	None
		Low (v3.0)
		High (v3.0)
		Single (v2.0)
		Multiple (v2.0)
Влияние на конфиденциальность	C	None
		Low (v3.0)
		High (v3.0)
		Partial (v2.0)
		Complete (v2.0)
Влияние на целостность	I	None
		Low (v3.0)
		High (v3.0)
		Partial (v2.0)
		Complete (v2.0)
Влияние на доступность	A	None
		Low (v3.0)
		High (v3.0)
		Partial (v2.0)
		Complete (v2.0)
Необходимость взаимодействия с пользователем (User Interaction)	UI	None (v3.0)
		Required (v3.0)
Границы эксплуатации (Scope)	S	Unchanged (v3.0)
		Changed (v3.0)

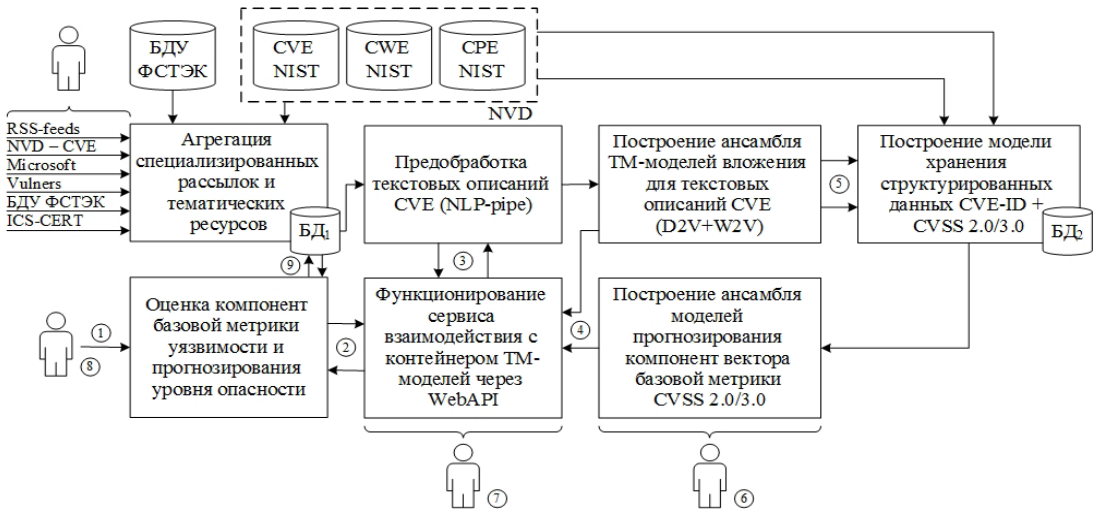

Рис. 1. Архитектура системы оценки опасности уязвимостей на основе технологий интеллектуального анализа данных

делей вложения на основе очищенных текстовых описаний уязвимостей с привязкой к ключу CVE-ID как взвешенная комбинация Doc2Vec и Word2Vec моделей. С помощью D2V и W2V моделей (5) формируется вектор вложений текстовых описаний для БД2, предназначенной для хранения структурированных данных {CVE-ID, вектор CVSS 2.0/3.0, Text Embedded Vector}.

На следующем шаге конструируется ансамбль моделей для прогнозирования компонент вектора базовой метрики CVSS 2.0/3.0.

Подготовленные модели прогнозирования вектора CVSS 2.0/3.0 помещаются в контейнер (4) для размещения на сервере для обработки запросов от пользователей системы через WebAPI.

Второй этап предполагает обработку запросов (1) по оценке уровня опасностей выявленных уязвимостей, для которой отсутствует оценка CVSS и размеченный вектор базовой метрики от специалиста по информационной безопасности (8), проводящего аудит ИС. Выполняется передача (9 и 2) текстовых описаний уязвимости и/или CVE-ID в одну из баз уязвимостей, а также проводится подготовка (3) его нормализованного и предобработанного текстового описания.

Поддержка адекватного состояния и дообучение моделей прогнозирования осуществляется инженером по работе с моделями машинного обучения (machine learning, ML) (6). Функционирование контейнера ML-моделей на сервере и обработка WebAPI запросов обеспечивается инженером поддержки Web-сервиса (7).

Таблица 2

Структура конвейера NLP-Pipe

Этап	Шаги	Действия	Инструменты
Предобработка	символьная фильтрация	Удаление нерелевантных символов, разворачивание сокращений, очистка от html-тегов	Набор из 40 регулярных выражений и библиотека BuitifulSoup
	токенизация	Разбивка текста на токены с помощью предобученной для русского языка нейросетевой модели	Razdel [13] (фреймворк Natasha)
	фильтрация нерелевантных токенов	Удаление дат, цифр, чисел, ссылок, сокращений	Регулярные выражения
Нормализация	лемматизация	Приведение слов в исходную форму с помощью предобученной нейросетевой модели	Morph (фреймворк Natasha)
Постобработка	частеречная фильтрация	Остаются только существительные, глаголы, прилагательные, наречия, местоимения	Morph (фреймворк Natasha)
	фильтрация на основе стоп-словарей	Фильтрация нерелевантных лемм с помощью составного стоп-словаря, включающего наиболее часто встречающиеся слова корпуса текстов	NLTK-russian, NLTK-english
	Формирование документа-строки	Объединение лемм в нормализованную строку-документ	

3. Анализ корпуса русскоязычных текстов – описаний уязвимостей БДУ ФСТЭК

Корпус текстов для анализа построен из 31384 агрегированных текстовых описаний уязвимостей на русском языке из БДУ ФСТЭК России. Составное текстовое поле включает данные о характеристике уязвимости и вариантах ее эксплуатации. Структура конвейера NLP-Pipe для обработки данных представлена в таблице 2.

Предварительный анализ корпуса текстов позволит оценить структуру корпуса и возможности применения моделей для построения предикторов. С помощью библиотеки Gensim выполним частотный анализ и оценку длины отдельных текстовых документов (рис. 2).

Далее выполним тематическое моделиро-

Рис. 2. Распределение количества слов в документах

вание на основе алгоритма латентного размещения Дирихле (LDA), которое позволит оценить возможность представления текстовых документов в виде смеси автоматически выделенных тем, и привязкой каждого слова к одной из них. Тематическая модель позволяет оценить структурированность текстов и потенциал их группировки по степени семантической близости. Использован вариант LDA на основе иерархической байесовской модели: на первом уровне – компоненты модели соответствуют «темам»; на втором уровне – мультиномиальной переменной с априорным распределением Дирихле, которые задают «распределение тем» в документе. Используются значения матрицы близости, основанной на частотных характеристиках документов и лексических единиц для первых четырех выделенных тем, что позволяет оценить словарный состав и частотное распределение слов для каждой из них (рис. 3).

Сложность (обобщающую способность) модели LDA составляет 5,926, а ее когерентность (мера интерпретируемости – оценка согласованности темы) 0,459, что позволяет

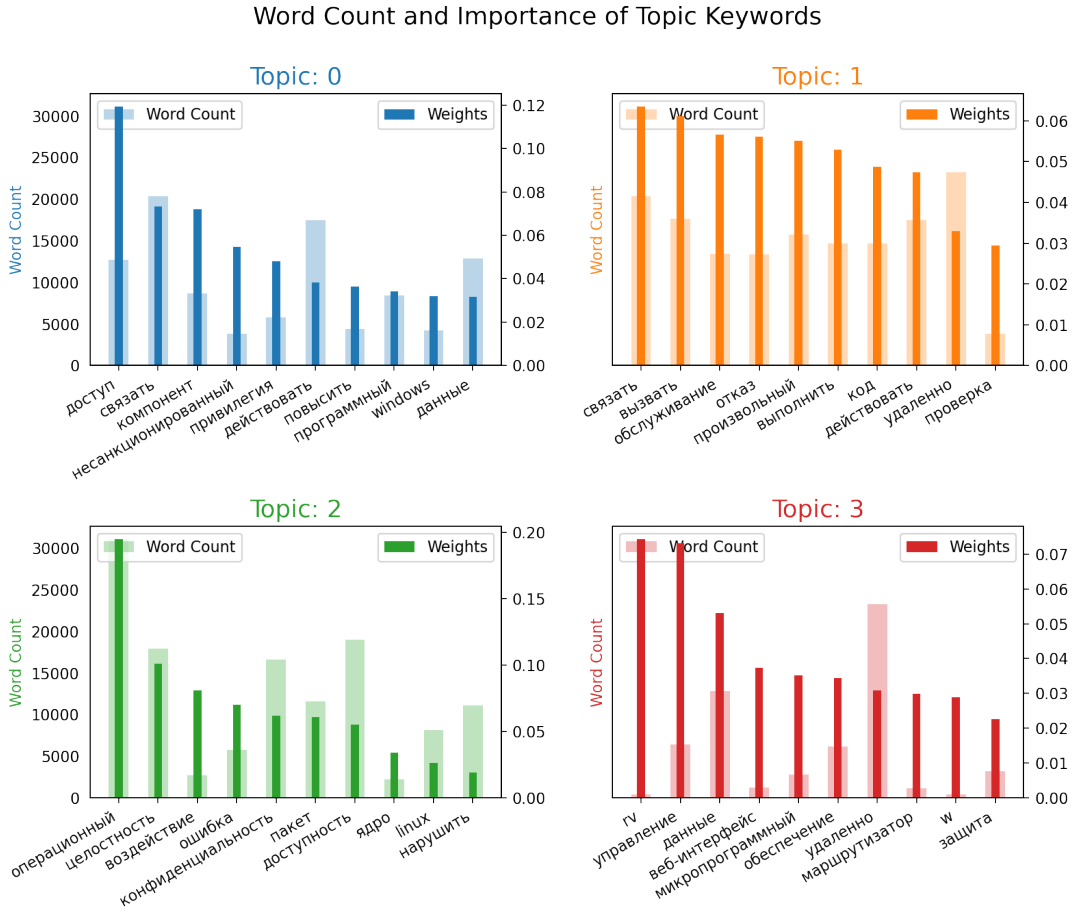

Рис. 3. Частотные характеристики первых четырех выделенных тем

сделать вывод о наличии структуры у корпуса текстов и возможности построения предикторов, реализующих задачу классификации по компонентам вектора метрики CVSS 2.0/3.0. С помощью t-distributed stochastic neighbor embedding, (стохастическое вложение соседей с распределением Стьюдента t-SNE) выполним понижение размерности

признакового пространства и визуализацию в пространстве двух переменных распределения документов по первым 4 темам (рис. 4). Компактные группы объектов хорошо отделимы друг от друга, однако, наличие характерных выбросов у каждой группы требует дальнейшего анализа и изменения алгоритма постфильтрации на основе расширяемого стоп-словаря, но не препятствует построению предикторов.

Далее для формализации признаков строится нейросетевая модель векторного вложения для текстовых документов Distributed memory (PV-DM) Doc2Vec [14] (таблица 3).

Для каждого документа корпуса с помощью обученной D2V модели строится вектор

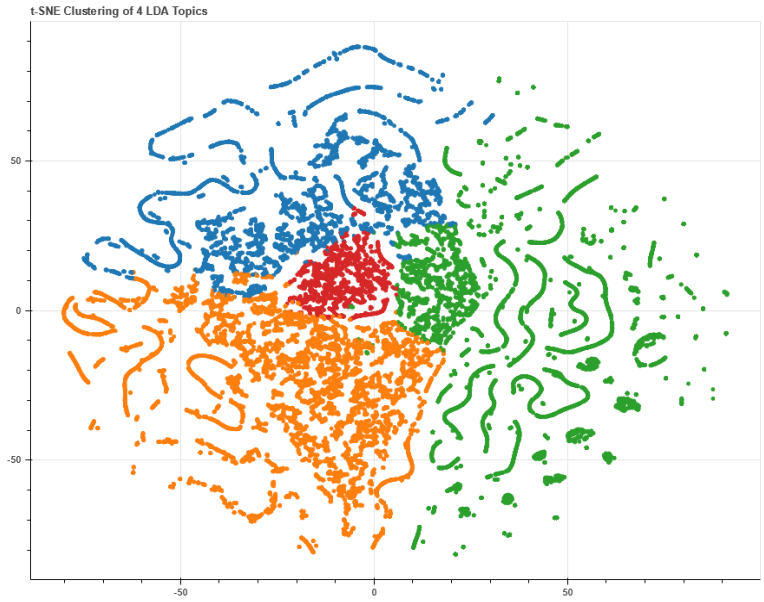

Рис. 4. t-SNE визуализация распределения для четырех основных тем

Таблица 3

Параметры Distributed memory (PV-DM) Doc2Vec Model

Параметр	Значение
Размерность вектора признаков	100
Размер окна анализа	5
Минимальная частота встречаемости слова для включения в модель	2
Количество эпох обучения	100

формальных признаков, на основе которого может быть оценена семантическая близость документов как косинус мера расстояния между векторами [15]. Это позволяет выполнять более качественный по сравнению с частотно-словарным (TF-IDF) поиск наиболее близких по смыслу документов. Предварительно рассчитанная разреженная матрица попарных расстояний позволяет существенно ускорить процедуру поиска и группировки уязвимостей. Пример поиска семантически близких описаний уязвимостей представлен в таблице 4.

4. Экспериментальная оценка опасности уязвимостей на основе технологий интеллектуального анализа данных

Для оценки BaseScore CVSS 2.0 рассмотрим два сценария:

– построение ансамбля предикторов для оценки отдельных значений компонент вектора (AV, AC, Au, C, I, A) по формализованному текстовому описанию с последующим расчетом оценки уровня опасности (таблица 5);

– построение модели регрессии для непосредственной оценки результирующего значения по формализованному текстовому описанию.

Построение ансамбля предикторов выполнено для 75% доступных документов с формальным вектором признаков, сформированным с помощью D2V модели. Оптимизация гиперпараметров используемых моделей предикторов выполнена с помощью процедуры перебора по сетке (GridSearch) с применением перекрестной проверки с разбие-

Таблица 4

Семантически близкие текстовые описания уязвимостей в порядке убывания косинус-меры

№	Документ	Мера близости
0	Уязвимость микропрограммного обеспечения программируемого логического контроллера Schneider Electric Modicon Quantum, позволяющая злоумышленнику получить авторизованный доступ к устройству. Микропрограммное обеспечение модуля 140NOE77111 контроллера Schneider Electric Modicon Quantum содержит множество пар логин: пароль, предустановленных по умолчанию. Это позволяет любому пользователю, имеющему доступ к устройству по протоколу FTP, получить авторизованный доступ к устройству	1
1	Уязвимость FTP-сервера микропрограммного обеспечения программируемых логических контроллеров Schneider Electric Modicon Premium, Modicon Quantum, Modicon M340 и Modicon BMXNOR0200, позволяющая нарушителю получить доступ к устройству. Уязвимость FTP-сервера микропрограммного обеспечения программируемых логических контроллеров Schneider Electric Modicon Premium, Modicon Quantum, Modicon M340 и Modicon BMXNOR0200 связана с использованием предустановленных учетных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к устройству	0,6742
2	Уязвимость микропрограммного обеспечения устройства SIEMENS LOGO!8, связанная с неправильным контролем доступа, позволяющая нарушителю получить доступ к устройству. Уязвимость микропрограммного обеспечения программируемого логического контроллера SIEMENS LOGO!8 связана с неправильным контролем доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, использовать перехваченный идентификатор сессии для доступа к устройству (даже после окончания сессии легитимным пользователем)	0,6724
…	…	…
25	Уязвимость микропрограммного обеспечения программируемого логического контроллера Modicon, связанная с раскрытием информации, позволяющая нарушителю получить доступ к конфиденциальной информации. Уязвимость микропрограммного обеспечения программируемого логического контроллера Modicon связана с раскрытием информации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получить доступ к конфиденциальной информации протокола SNMP при чтении блоков памяти контроллера с использованием протокола Modbus	0,5761

нием на 5 блоков. Параметры подбора приведены в таблице 5.

Результаты работы каждого предиктора на обучающей и тестовой выборках (25% исходных документов) для всех компонент вектора базовой метрики приведены в таблице 6 и на рис. 5.

Оценка классификаторов выполнена с помощью следующих метрик:

– Accuracy (точность) показывает долю правильных классификаций.

– Precision (точность) показывает долю объектов класса среди всех объектов, выделенных классификатором

– Recall (полнота) отражает долю найденных объектов класса от общего числа объектов класса.

– F_1 – среднее гармоническое Precision и Recall.

Второй сценарий подразумевает построение модели регрессии на основе ансамбля решающих деревьев (Random Forest) с оптимизацией гиперпараметров с помощью процедуры перебора по сетке (GridSearch) с применением перекрестной проверки с разбиением на 5 блоков. Результирующая модель ансамбля включает 500 решающих деревьев с максимальной глубиной 8.

Для обучающей выборки среднеквадратичная ошибка (Root Mean Square Error) составила 0,669, а для тестовой – 1,316.

Прогноз оценки уровня опасности уязвимости для 50 примеров из обучающей выборки и 50 примеров тестовой выборки представлен на рис. 6, где маркер «круг» – исходное значение, маркер «крест» – предсказанного, ось ординат – уровень опасности уязвимости.

5. Анализ результатов

Анализ таблицы 4 показывает, что выделенные уязвимости семантически близки к исходному документу, предварительно построенная матрица попарных расстояний близости описаний позволяет за константное время выполнять поиск близких описаний уязвимостей и их ранжирование для представления специалисту, проводящему аудит защищенности системы.

Таблица 5

Параметры моделей предикторов

Классификатор	Пространство гиперпараметров		Параметры обучения		
			Моделей	K-fold cross-validation	Среднее время, m
SGD (SVM) Классификатор на основе машины опорных векторов	tol (точность)	1e-3	576	5	35
	loss (функция потерь)	hinge, modified_huber			
	max_iter (максимальное количество и итераций)	10, 100, 1000			
	alpha (коэффициент регуляризации)	1e-6, 1e-4, 1e-2, 1e-1			
	learning_rate (алгоритм изменения градиентного шага)	optimal, invscaling			
	eta0 (начальный градиентный шаг)	1e-5, 1e-3, 1e-1, 1			
	penalty (метод регуляризации)	l1, l2, elasticnet			
SGD (LR) Классификатор на основе модели линейной регрессии	tol	1e-3	288	5	19,3
	loss	hinge, modified_huber			
	max_iter	10, 100, 1000			
	alpha	1e-6, 1e-4, 1e-2, 1e-1			
	learning_rate	optimal, invscaling			
	eta0	1e-5, 1e-3, 1e-1, 1			
	penalty	l1, l2, elasticnet			
KNeighbors Классификатор k ближайших соседей	n_neighbors (количество соседей для использования по умолчанию для запросов k соседей)	5	12	5	3,9
	weights (весовая функция, используемая в прогнозировании)	distance			
RandomForest Классификатор на основе комитета случайных деревьев решений	max_depth (максимальная глубина дерева. Если None, то узлы расширяются до тех пор, пока все листья не станут чистыми или пока все листья не будут содержать менее min_samples_split выборок)	None	60	5	26,3
	min_samples_split (минимальное количество выборок, необходимое в узле, чтобы вызвать расщепление узла)	2			
	n_estimators (количество деревьев в ансамбле)	500			

Таблица 6

Результаты работы предикторов на обучающей и тестовой выборках

Компонент	Классификатор	Обучающая выборка				Тестовая выборка			
		F1	Accuracy	Precision	Recall	F1	Accuracy	Precision	Recall
AV	SGD (SVM)	0,948	0,958	0,939	0,958	0,948	0,958	0,939	0,958
	SGD (LR)	0,744	0,804	0,818	0,804	0,744	0,804	0,816	0,804
	KNeighbors	1,000	1,000	1,000	1,000	0,963	0,965	0,964	0,965
	RandomForest	1,000	1,000	1,000	1,000	0,948	0,953	0,955	0,953
AC	SGD (SVM)	0,588	0,645	0,590	0,645	0,580	0,640	0,581	0,640
	SGD (LR)	0,555	0,652	0,594	0,652	0,552	0,650	0,584	0,650
	KNeighbors	1,000	1,000	1,000	1,000	0,759	0,766	0,759	0,766
	RandomForest	1,000	1,000	1,000	1,000	0,737	0,764	0,778	0,764
Au	SGD (SVM)	0,786	0,838	0,779	0,838	0,782	0,836	0,770	0,836
	SGD (LR)	0,771	0,843	0,710	0,843	0,771	0,843	0,710	0,843
	KNeighbors	1,000	1,000	1,000	1,000	0,898	0,901	0,896	0,901
	RandomForest	0,988	0,989	0,989	0,989	0,872	0,889	0,881	0,889
C	SGD (SVM)	0,661	0,673	0,665	0,673	0,652	0,665	0,657	0,665
	SGD (LR)	0,506	0,581	0,606	0,581	0,495	0,571	0,582	0,571
	KNeighbors	1,000	1,000	1,000	1,000	0,770	0,773	0,771	0,773
	RandomForest	1,000	1,000	1,000	1,000	0,772	0,779	0,781	0,779
I	SGD (SVM)	0,700	0,707	0,698	0,707	0,694	0,701	0,692	0,701
	SGD (LR)	0,579	0,637	0,677	0,637	0,569	0,630	0,671	0,630
	KNeighbors	1,000	1,000	1,000	1,000	0,778	0,783	0,778	0,783
	RandomForest	1,000	1,000	1,000	1,000	0,773	0,782	0,779	0,782
A	SGD (SVM)	0,583	0,660	0,617	0,660	0,581	0,658	0,612	0,658
	SGD (LR)	0,508	0,608	0,562	0,608	0,516	0,615	0,583	0,615
	KNeighbors	1,000	1,000	1,000	1,000	0,780	0,787	0,780	0,787
	RandomForest	1,000	1,000	1,000	1,000	0,770	0,785	0,783	0,785

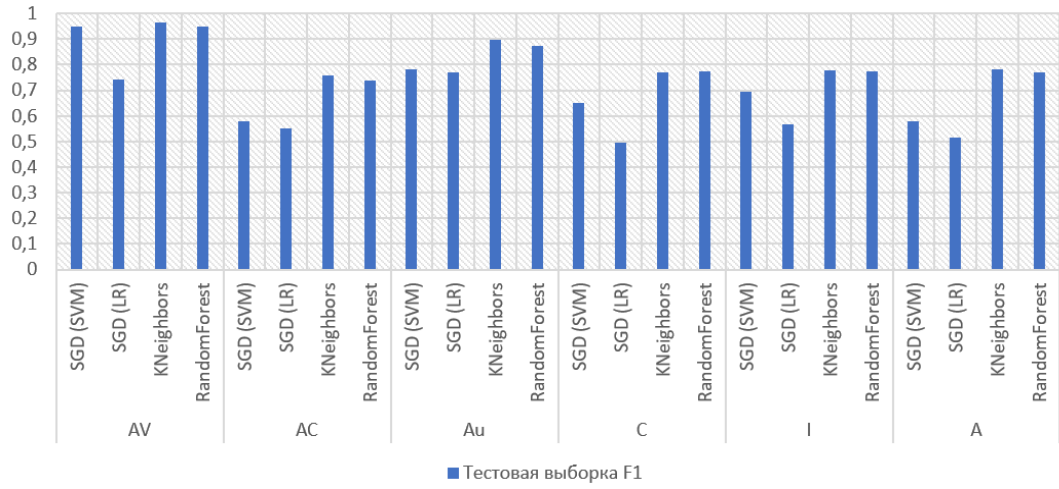

Рис. 5. Оценка F1 меры для тестовой выборки по каждому классификатору и компоненту метрики

Анализ таблицы 6 показывает, что ансамбль предикторов позволяет получить оценку компонент вектора базовой метрики новых уязвимостей на уровне значения меры F_1 = 0,70-0,75 для тестовой выборки, что свидетельствует о хорошей обобщающей способности предлагаемого решения.

Модель регрессии на основе ансамбля решающих деревьев позволяет непосредственно оценивать уровень опасности уязвимости, но без определения компонент базовой метрики.

Заключение

Предлагаемый подход основан на применении технологий интеллектуального анализа описаний уязвимостей на естественном

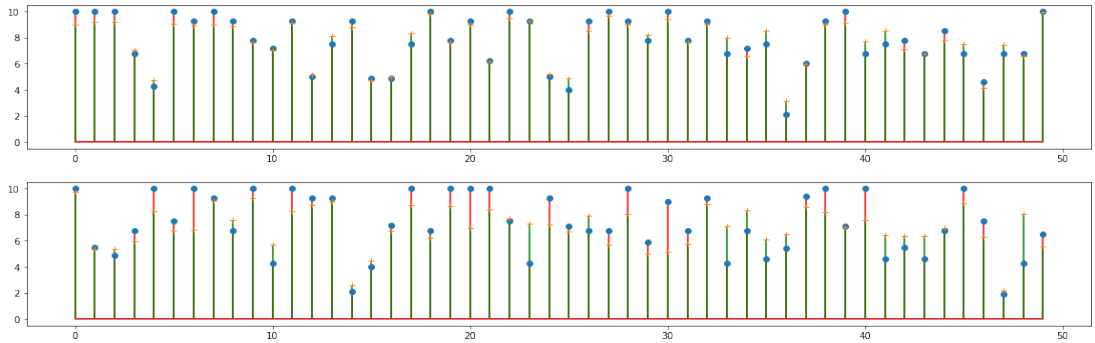

Рис. 6. Прогноз оценки уровня опасности уязвимости для 50 примеров из обучающей выборки (вверху) и 50 примеров тестовой выборки (внизу).

языке. Отличительной особенностью является использование построение модели вложения слов и описаний уязвимостей и композиции классификаторов, выполняющих оценку компонент вектора метрики уязвимости согласно стандарту CVSS. Применение предлагаемого подхода позволит получить оценку метрики опасности (и ее компонент) зарегистрированной уязвимости на основе анализа семантической близости текстового описания к уже имеющимся в реестре записям.

Практическая значимость обусловлена повышением эффективности (точности и оперативности) оценки метрик опасности уязвимостей с возможностью интеграции в систему аудита и инвентаризации для оперативного принятия мер по защите от новых уязвимостей.

Литература

1. Claroty Biannual ICS Risk & Vulnerability Report: 2H 2020. [Электронный ресурс] URL: https://security.claroty.com/biannual-ics-risk-vulnerability-report-2H-2020 (дата обращения: 10.04.2021)

2. Feutrill A. et al. The effect of common vulnerability scoring system metrics on vulnerability exploit delay // 2018 Sixth International Symposium on Computing and Networking (CANDAR). IEEE, 2018. P. 1–10.

3. Chen H. et al. VEST: A System for Vulnerability Exploit Scoring & Timing // IJCAI, 2019. P. 6503–6505.

4. Urbanska M., Ray I., Home A.E., Roberts M. Structuring a Vulnerability Description for Comprehensive Single System Security Analysis // RMCWiC'2012. [Электронный ресурс]. URL: www.cs.colostate.edu/psysec/papers/urbanskaRMCWiC`2012.pdf (дата обращения: 10.04.2021)

5. Spanos G., Angeis L., Toloudis D. Assessment of Vulnerability Severity using Text Mining // Proceedings of the 21st Pan-Hellenic Conference, Sept.2017, Larissa, Greece. P. 1–6.

6. Han Z., Li X., Xing Z., LiuH., Feng Z. Learning to Predict Severity of Software Vulnerability Description // Proceedings of the 2017 International Conference on Software Maintenance and Evolution (ICSME), Shanghai, China, Nov.2017. P. 125–136.

7. Lee Y., Shin S. Toward Semantic Assessment of Vulnerability Severity: A Text Mining Approach // Proceedings of ACM CIKM Workshop (EYRE' 18), 2018. [Электронный ресурс]. URL: https://www.CEUR-WS.org/Vol1-2482/papers.pdf (дата обращения: 10.04.2021)

8. Datta P. et al. Cyber-Attack Consequence Prediction //arXiv preprint arXiv:2012.00648. 2020.

9. Elbaz C., Rilling L., Morin C. Fighting N-day vulnerabilities with automated CVSS vector prediction at disclosure // Proceedings of the 15th International Conference on Availability, Reliability and Security, 2020. P. 1–10.

10. Khazaei A., Ghasemzadeh M., Derhami V. An automatic method for CVSS score prediction using vulnerabilities description // Journal of Intelligent & Fuzzy Systems, 2016. Vol. 30, No. 1. P. 89–96.

11. Лаврентьев А.М. и др. Сравнительный анализ специальных корусов текстов для задач безопасности // Вопросы кибербезопасности. 2020. № 3(37). С. 54–60.

12. Селифанов В.В., Юракова Я.В., Картамов И.Н. Методика автоматизированного выявления взаимосвязей уязвимостей и угроз безопасности информации в информационных системах // Интерэкспо Гео-Сибирь. 2018. С. 271–276.

13. Rule-based token, sentence segmentation for Russian language [Электронный ресурс] URL: https://github.com/natasha/razdel (дата обращения: 10.04.2021)

14. Mendsaikhan O. et al. Identification of cybersecurity specific content using the Doc2Vec language

model // 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC). IEEE, 2019. Vol. 1. P. 396–401.

15. Бондарчук Д.В. Векторная модель представления знаний на основе семантической близости термов // Вестник ЮрГУ. Серия: Вычислительная математика и информатика. 2017. Т. 7. С. 73–83.

References

1. Claroty Biannual ICS Risk & Vulnerability Report: 2H 2020. Available at: https://security.claroty.com/biannual-ics-risk-vulnerability-report-2H-2020 (accessed April 10, 2021).

2. Feutrill A. et al. The effect of common vulnerability scoring system metrics on vulnerability exploit delay // 2018 Sixth International Symposium on Computing and Networking (CANDAR). IEEE, 2018. pp. 1-10.

3. Chen H. et al. VEST: A System for Vulnerability Exploit Scoring & Timing // IJCAI, 2019. pp. 6503-6505.

4. Urbanska M., Ray I., Home A.E., Roberts M. Structuring a Vulnerability Description for Comprehensive Single System Security Analysis // RMCWiC'2012. Available at: www.cs.colostate.edu/psysec/papers/urbanskaRMCWiC`2012.pdf (accessed April 10, 2021).

5. Spanos G., Angeis L., Toloudis D. Assessment of Vulnerability Severity using Text Mining // Proceedings of the 21st Pan-Hellenic Conference, Sept.2017, Larissa, Greece. pp. 1-6.

6. Han Z., Li X., Xing Z., LiuH., Feng Z. Learning to Predict Severity of Software Vulnerability Description // Proceedings of the 2017 International Conference on Software Maintenance and Evolution (ICSME), Shanghai, China, Nov.2017. pp. 125-136.

7. Lee Y., Shin S. Toward Semantic Assessment of Vulnerability Severity: A Text Mining Approach // Proceedings of ACM CIKM Workshop (EYRE ' 18), 2018. Available at: https://www.CEUR-WS.org/Vol1-2482/papers.pdf (accessed April 10, 2021).

8. Datta P. et al. Cyber-Attack Consequence Prediction //arXiv preprint arXiv:2012.00648. 2020.

9. Elbaz C., Rilling L., Morin C. Fighting N-day vulnerabilities with automated CVSS vector prediction at disclosure // Proceedings of the 15th International Conference on Availability, Reliability and Security, 2020. pp. 1-10.

10. Khazaei A., Ghasemzadeh M., Derhami V. An automatic method for CVSS score prediction using vulnerabilities description // Journal of Intelligent & Fuzzy Systems, 2016. Vol. 30, no. 1. pp. 89-96.

11. Lavrent'ev A.M. i dr. Sravnitel'nyj analiz special'nyh korusov tekstov dlya zadach bezopasnosti // Voprosy kiberbezopasnosti. 2020. № 3(37). S. 54-60.

12. Selifanov V.V., YUrakova YA.V., Kartamov I.N. Metodika avtomatizirovannogo vyyavleniya vzaimosvyazej uyazvimostej i ugroz bezopasnosti informacii v informacionnyh sistemah // Interekspo Geo-Sibir'. 2018. S. 271-276.

13. Rule-based token, sentence segmentation for Russian language Available at: URL: https://github.com/natasha/razdel (accessed April 10, 2021).

14. Mendsaikhan O. et al. Identification of cybersecurity specific content using the Doc2Vec language model // 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC). IEEE, 2019. Vol. 1. pp. 396-401.

15. Bondarchuk D.V. Vectornaya model' predstavleniya znanij na osnove semanticheskoj blizosti termov // Vestnik YUrGU. Seriya: Vychislitel'naya matematika i informatika. 2017. T. 6, S. 73-83.

ВАСИЛЬЕВ Владимир Иванович, доктор технических наук, профессор кафедры вычислительной техники и защиты информации ФГБОУ ВО «Уфимский государственный авиационный технический университет», Россия, 450008, г. Уфа, ул. К.Маркса, 12. E-mail: vasilyev@ugatu.ac.ru

ВУЛЬФИН Алексей Михайлович, кандидат технических наук, доцент кафедры вычислительной техники и защиты информации, ФГБОУ ВО «Уфимский государственный авиационный технический университет», Россия, 450008, г. Уфа, ул. К.Маркса, 12. E-mail: vulfin.alexey@gmail.com

КИРИЛЛОВА Анастасия Дмитриевна, аспирант кафедры вычислительной техники и защиты информации, ФГБОУ ВО «Уфимский государственный авиационный технический университет», Россия, 450008, г. Уфа, ул. К.Маркса, 12. E-mail: kirillova.andm@gmail.com

НИКОНОВ Андрей Владимирович, аспирант кафедры вычислительной техники и защиты информации, ФГБОУ ВО «Уфимский государственный авиационный технический университет», Россия, 450008, г. Уфа, ул. К.Маркса, 12. E-mail: nikonovandrey1994@gmail.com

VASILYEV Vladimir, Dr. Sc. (Eng.), Professor of the Department «Computer Engineering and Information Security», Ufa State Aviation Technical University». 12, K. Marx Str., Ufa, 450008, Russia. E-mail: vasilyev@ugatu.ac.ru

VULFIN Alexey, PhD (Cand. of Sc.) Ass. Professor of the Department «Computer Engineering and Information Security», Ufa State Aviation Technical University. 12, K. Marx Str., Ufa, 450008, Russia. E-mail: vulfin.alexey@gmail.com

KIRILLOVA Anastasiya, Postgrad. Student of the Department «Computer Engineering and Information Security», Ufa State Aviation Technical University. 12, K. Marx Str., Ufa, 450008, Russia. E-mail: kirillova.andm@gmail.com

NIKONOV Andrey, Postgrad. Student of the Department «Computer Engineering and Information Security», Ufa State Aviation Technical University. 12, K. Marx Str., Ufa, 450008, Russia. E-mail: nikonovandrey1994@gmail.com

УДК 004.896 + 004.056.5 Вестник УрФО № 2(40) / 2021, с. 44–58

Рагозин А. Н.

DOI: 10.14529/secur210205

ФОРМИРОВАНИЕ ПРОГНОЗА МНОГОКОМПОНЕНТНЫХ ВРЕМЕННЫХ РЯДОВ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ ЦИФРОВОЙ ФИЛЬТРАЦИИ И ПРОГНОЗИРУЮЩЕГО АВТОКОДИРОВЩИКА С ЦЕЛЬЮ ОБНАРУЖЕНИЯ АНОМАЛИЙ В РАБОТЕ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ КИБЕРАТАК

Эффективность современных сложных автоматизированных систем управления технологическими процессами (АСУ ТП) складывается из показателей качества формирования в подобных системах управленческих решений и воздействий, а также способности сохранения устойчивого функционирования в условиях сильной неопределенности изменяющейся внешней среды, например, в следствии воздействия кибератак, как на информационном уровне, так и на кибернетическом уровне в АСУ ТП. Динамические временные ряды данных, отражающие процессы, протекающие в современных сложных АСУ ТП представляют результат взаимодействия многих подсистем и поэтому являются сложными многокомпонентными временными рядами. С целью обнаружения аномалий и повышения качества прогнозирования динамических многокомпонентных временных рядов данных, наблюдаемых с сенсоров в АСУ ТП, предлагается формировать прогноз в различных временных масштабах (краткосрочный, среднесрочный, долго-

срочный) развивающейся ситуации в АСУ ТП. При возникновении аномалий в работе АСУ ТП будут происходить структурные изменения в сигнале ошибки формируемого прогноза, в результате анализа этих структурных изменений ошибки прогноза, собственно происходит детектирование (обнаружение) аномалий в наблюдаемых процессах АСУ ТП. Структурный анализ многокомпонентного временного ряда и соответственно формирование архитектуры искусственной нейронной сети позволяют формировать прогноз в различных временных масштабах. Предлагаемый подход формирования прогноза в различных временных масштабах, позволит обнаруживать в множестве наблюдаемых временных рядов данных АСУ ТП аномалии раздельно по их различным динамическим характеристикам, что повышает эффективность управления устойчивостью функционирования АСУ ТП в условиях воздействия кибератак.

Ключевые слова: *цифровая фильтрация, искусственная нейронная сеть, многокомпонентный прогноз, прогнозирующий автоэнкодер, автоматизированная система управления технологическими процессами, кибератаки.*

Ragozin A. N.

FORMATION OF A FORECAST OF MULTICOMPONENT TIME SERIES OF DATA USING DIGITAL FILTERING METHODS AND A PREDICTIVE AUTOENCODER IN ORDER TO DETECT ANOMALIES IN THE OPERATION OF AUTOMATED CONTROL SYSTEMS FOR TECHNOLOGICAL PROCESSES UNDER THE INFLUENCE OF CYBERATTACKS

The effectiveness of modern complex automated process control systems (APCS) consists of the quality indicators of the formation in such systems of managerial decisions and influences,

as well as the ability to maintain stable functioning in conditions of strong uncertainty in a changing external environment, for example, because of the impact of cyberattacks, as at the information level and at the cybernetic level in the APCS. Dynamic time series of data reflecting the processes occurring in modern complex APCS represent the result of the interaction of many subsystems and therefore are complex multicomponent time series. In order to detect anomalies and improve the quality of forecasting dynamic multicomponent time series of data observed from sensors in the APCS, it is proposed to form a forecast at various time scales (short-term, medium-term, long-term) of the developing situation in the APCS. In the event of anomalies in the operation of the automated process control system, structural changes will occur in the error signal of the generated forecast; as a result of the analysis of these structural changes in the forecast error, in fact, anomalies are detected in the observed processes of the APCS. Structural analysis of a multicomponent time series and, accordingly, the formation of the architecture of artificial neural networks make it possible to form a forecast at different time scales. The proposed approach to the formation of a forecast in different time scales will allow detecting anomalies in the set of observed time series of APCS data separately according to their different dynamic characteristics, which increases the efficiency of managing the stability of the functioning of the APCS under cyberattacks.

Keywords: *digital filtering, artificial neural network, multicomponent forecast, predictive autoencoder, automated process control system, cyberattacks.*

Введение

Эффективность управления информационной безопасностью в современных сложных автоматизированных системах управления технологическими процессами (АСУ ТП) складывается из показателей качества формирования в подобных системах управленческих решений и воздействий, а также способности сохранения устойчивого функционирования в условиях сильной неопределённости изменяющейся внешней среды, например, в следствии воздействия кибератак, как на информационном уровне, так и на кибернетическом уровне в АСУ ТП. Воздействие кибератак проявляется в виде аномалий (неожидаемого изменения свойств) динамических рядов данных, отражающих работу АСУ ТП. Важной является задача оперативного обнаружения аномалий в работе АСУ ТП в условиях воздействия кибератак.

Современные АСУ ТП состоят из многих подсистем, поэтому процессы, протекающие в них и отражаемые в наблюдаемых потоках данных, являются сложными многокомпонентными процессами. Потоки данных в таких сложных автоматизированных системах можно упорядочить во временные ряды данных и, соответственно осуществлять прогноз сложных многокомпонентных временных рядов данных в различных временных масштабах (краткосрочный, среднесрочный, долгосрочный). Для реализации прогноза в различных временных масштабах необходим структурный анализ многокомпонентного временного ряда и соответственно, формирование масштабируемого прогноза [1, 2].

Атаки вызывают аномалии (то есть, неожидаемое изменение) в поведении наблюдаемых процессов (в динамике наблюдаемых временных рядов данных) при работе АСУ ТП. Технология прогнозирования играет важную роль при построении систем обнаружении (детектирования) аномалий в динамических потоках данных АСУ ТП [3-5]. Предлагаемый подход формирования прогноза в различных временных масштабах, позволит обнаруживать в множестве наблюдаемых временных рядов данных АСУ ТП аномалии раздельно по их различным динамическим характеристикам, что повышает эффективность управления устойчивостью функционирования АСУ ТП в условиях сильной неопределённости изменяющейся внешней среды, а также, в следствии воздействия кибератак на АСУ ТП.

Методы прогнозирования динамических рядов данных, рассмотрены в работах [6-10].

Методы обнаружения аномалий с использованием искусственных нейронных сетей (ИНС) рассмотрены в работах [11-19].

Из анализа российских и зарубежных источников следует, что задача формирования масштабируемого прогноза на различных временных интервалах по наблюдаемым сложным многокомпонентным временным рядам в настоящее время не имеет завершенного решения. В настоящей работе рассматриваются этапы и результат построения про-

гноза многокомпонентных временных рядов, наблюдаемых в АСУ ТП.

1. Этапы построения прогноза многокомпонентного динамического временного ряда АСУ ТП

Динамические потоки данных, наблюдаемые в АСУ ТП представляют собой многокомпонентные временные ряды данных.

Для построения многокомпонентного (масштабируемого) прогноза в различных временных масштабах необходима реализация первого этапа – применение технологии цифровой обработки сигналов (ЦОС) для разложения сложного многокомпонентного временного ряда на отдельные базовые компоненты (структурный анализ многокомпонентного временного ряда, для наблюдаемого множества всех временных рядов, отражающих работу АСУ ТП).

При реализации второго этапа, происходит формирование архитектуры модульной ИНС для формирования прогноза в соответствии со структурой прогнозируемого многокомпонентного временного ряда (для каждого отдельного временного ряда, из наблюдаемого множества всех временных рядов, отражающих работу АСУ ТП). При этом, для каждой базовой компоненты прогнозируемого многокомпонентного временного ряда, в соответствии с их динамическими характеристиками формируются отдельные прогнозы с различным по длительности временным горизонтом. Более «медленные и инерционные» базовые компоненты допускают в результате более длительной автокорреляции, соответственно более длительный прогноз на больший интервал времени вперёд.

При реализации третьего этапа, по полученным прогнозам, отдельных базовых компонент с различным временным горизонтом, формируется завершённый масштабируемый прогноз на различных временных интервалах, то есть прогноз исходного многокомпонентного временного ряда. Самый дальний горизонт прогнозирования исходного многокомпонентного временного ряда определяется самой медленной базовой компонентой. Самый ближний горизонт прогнозирования исходного многокомпонентного временного ряда определяется параметрами самой быстрой базовой компоненты.

Возможности сформированного масштабируемого прогноза в различных временных масштабах для обнаружения в множестве наблюдаемых временных рядов данных АСУ ТП аномалий раздельно по их различным динамическим характеристикам рассмотрены в работах [3, 5].

2. Формирование структуры прогнозирующего модуля для построения прогноза динамического временного ряда данных АСУ ТП

Для формирования прогноза, каждой отдельной компоненты прогнозируемого многокомпонентного временного ряда в работе [20] предложен и рассмотрен прогнозирующий автокодировщик (автоэнкодер, PAE), позволяющий, кроме восстановления на выходе PAE входного сигнала, или части входного сигнала, также формировать на выходе PAE прогнозируемые отсчеты входного сигнала на заданное количество временных шагов «вперед». Показано [20], что использование PAE повышает точность результата прогнозирования исследуемого сигнала.

На рисунках 1-3 представлены типовые структуры ИНС автокодировщиков (автоэнкодеров, AE)).

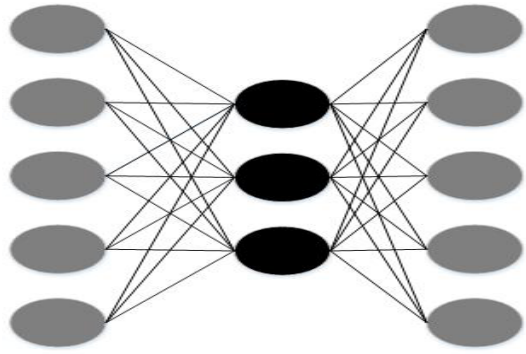

Рис. 1. Типовая структура ИНС автокодировщика (автоэнкодера, AE)

Типовой автокодировщик (автоэнкодер) (рис.1) реализуется в виде ИНС прямого распространения, восстанавливающей входной сигнал на выходе ИНС, при этом размер внутреннего слоя ИНС меньше размерности входного и выходного (восстановленного) сигнала.

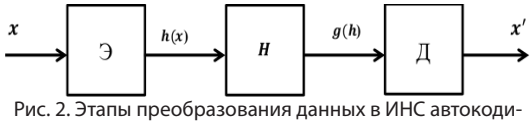

Рис. 2. Этапы преобразования данных в ИНС автокодировщике

На рисунке 2 отображены этапы преобразования данных в автокодировщике. На структурной схеме (рис.2) обозначено: входной сигнал x, выходной сигнал x', представляющий собой копию входного сигнала x. Авто-

кодировщик состоит из двух частей: энкодера и декодера. Энкодер переводит входной сигнал x в его представление (сжатый код): $h = g(x)$, а декодер восстанавливает сигнал x по его коду: $x = f(h)$ Обобщённая структурная схема автоэнкодера, содержащая несколько скрытых слоёв, представлена на рисунке 3.

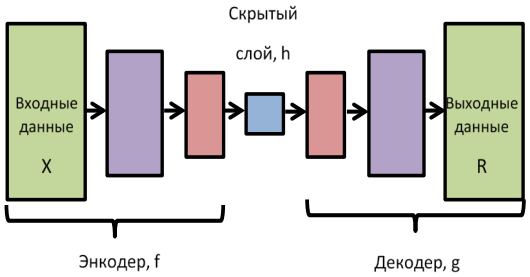

Рис. 3. Обобщённая структурная схема автокодировщика, содержащая несколько скрытых слоёв

Задача ИНС автоэнкодера, состоит в восстановлении, с сохранением наиболее важных свойств, входных данных x в качестве выходных данных x'.

Возможно модифицировать задачу выполняемую ИНС автокодировщика, добавив требование, чтобы кроме отображения входных данных x, в выходные данные x', с сохранением наиболее важных свойств входных данных x, дополнительно, также формировать в выходных данных x', прогнозируемые значения входных данных x. Предполагается, что возможность ИНС автокодировщика (автоэнкодера) при этом отбирать наиболее важные свойства входных данных x, приведёт к повышению качества формируемого прогноза входных данных x, содержащегося в восстанавливаемых автокодировщиком выходных данных x'.

На рисунке 4 отображено преобразование типовой структуры автокодировщика (AE) в структуру прогнозирующего автокодировщика (PAE). Белыми кружками обозначены добавленные прогнозируемые отсчёты входного сигнала x, сформированные в выходном сигнале x'.

На рис. 5а отображена структура прогнозирующего автокодировщика с формированием не симметричного прогноза входного сигнала, на рис. 5б отображено формирование только прогноза входного сигнала, при этом структура (рис. 5б) вырождается в структуру стандартного предиктора, формирующего на выходе только прогнозные значения входного сигнала.

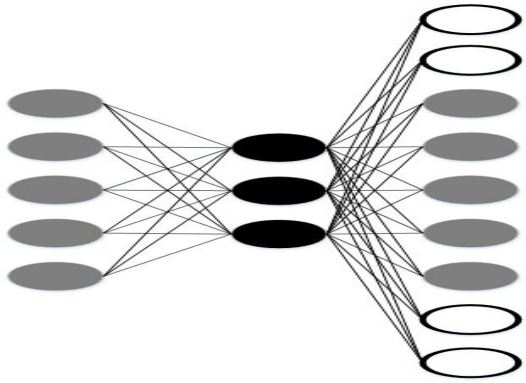

Рис. 4. Структура ИНС прогнозирующего автокодировщика (PAE)

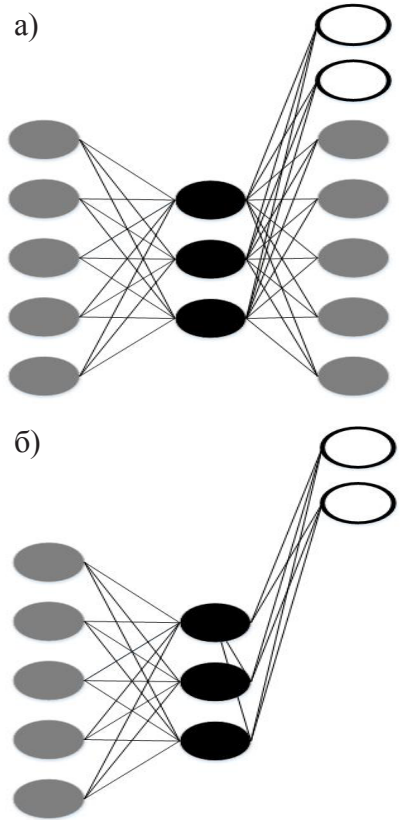

Рис. 5. Структура прогнозирующего автокодировщика с формированием не симметричного прогноза входного сигнала (а), структура стандартного предиктора входного сигнала (б)

Возможно сформировать модифицированную структуру прогнозирующего автокодировщика с формированием прогноза и одновременно с частичным восстановлением входного сигнала (то есть, части входного сигнала) (рис.6а), также с требованием реализовать дополнительное отображение входного сигнала в некоторый выходной сигнал с заданными свойствами (рис. 6б, заштрихованные кружки).

На рис. 7 представлена обобщённая

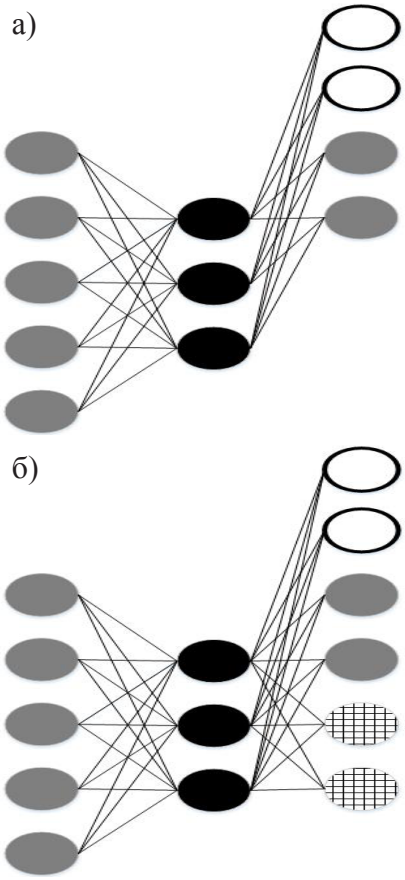

Рис. 6. Модифицированные структуры прогнозирующего автокодировщика

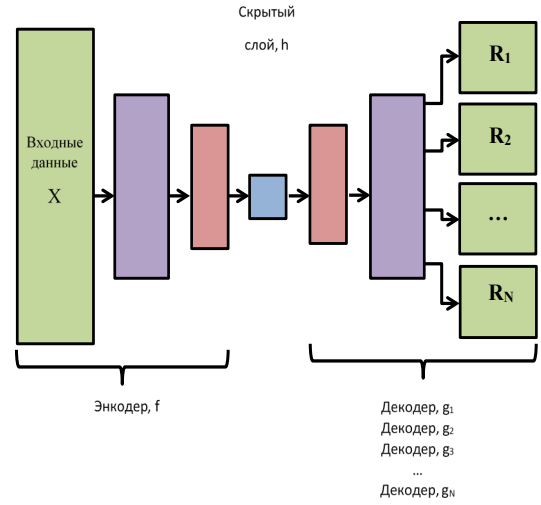

Рис. 7. Обобщённая структурная схема модифицированного автокодировщика, содержащая несколько скрытых слоёв

структура модифицированного прогнозирующего автокодировщика, содержащая несколько скрытых слоёв, результат модификации – одновременное формирование на выходе модифицированного автокодировщика различных отображений входного сигнала: полностью всего входного сигнала (что, является функцией стандартного автокодировщика) или только части входного сигнала, также требуемых прогнозных значений входного сигнала, также дополнительно возможно требование формирования набора различных отображений входного сигнала в требуемые выходные сигналы с заданными свойствами.

Модификация прогнозирующего автокодировщика, представленная на рис.7 позволяет реализовать управление качеством формируемого прогноза входного сигнала за счёт требования одновременной реализации множества дополнительных отображений входного сигнала, формируемых на выходе прогнозирующего автокодировщика (автоэнкодера, PAE) в требуемые выходные сигналы, обладающие различными требуемыми свойствами.

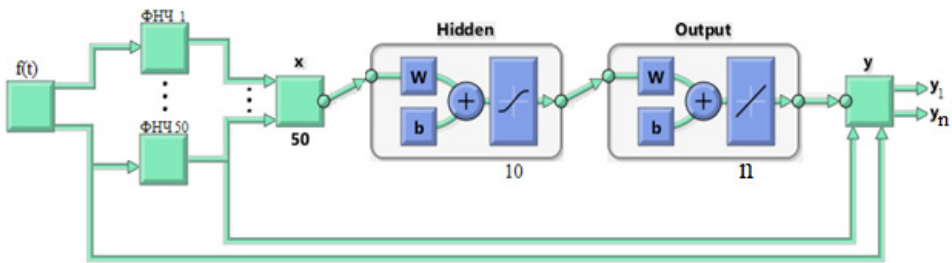

Рис. 8. Структурная схема прогнозирующего модуля: блок ЦОС и прогнозирующий блок с использованием ИНС

В работе [20] для прогнозирования сигналов предлагается применять прогнозирующий модуль, представленный на рис. 8, состоящий из последовательно соединенных блока ЦОС и прогнозирующего блока с использованием ИНС.

В прогнозирующем модуле (рис. 8) блок ЦОС состоит из гребенки цифровых фильтров нижних частот с конечной импульсной характеристикой (КИХ-ФНЧ). При этом на выходе гребенки КИХ-ФНЧ формируется набор отфильтрованных компонентов входного сигнала, далее, подаваемые на вход ИНС [20]. Целевыми отсчетами, подаваемыми на выход

ИНС при машинном обучении прогнозирующего модуля, являются целевые (прогнозируемые) отсчеты входного сигнала (впоследствии, итоговые результаты прогноза), Также, дополнительными целевыми отсчетами, подаваемыми на выход ИНС при машинном обучении прогнозирующего модуля являются дополнительные отсчеты, в виде выборки заданной длины из отсчетов исходного входного сигнала (то есть, со входа блока ЦОС), плюс дополнительно выборки заданной длины из отсчетов сигнала с входа ИНС (то есть, с выхода блока ЦОС). Дополнительно подаваемые на выход ИНС (при машинном обучении) целевые отсчёты, требуют кроме формирования требуемого прогноза, также дополнительное восстановление на выходе ИНС части исходного входного сигнала и части отсчётов сигналов с выхода гребенки КИХ-ФНЧ блока ЦОС. Прогнозирующий модуль, представленный на рис. 8 реализован в соответствии с модифицированной структурой прогнозирующего автокодировщика (автоэнкодера, PAE), отображённого на рис. 6б. Более подробное описание и исследование прогнозирующего модуля, (рис. 8) приведено в работе [20].

3. Результаты исследования качества формируемого прогноза прогнозирующим модулем, реализованным в виде модифицированного прогнозирующего автокодировщика (автоэнкодера)

Проведём сравнение качества прогноза исследуемого сигнала, формируемого стандартным предиктором исследуемого сигнала (рис. 5б) и модифицированным прогнозирующим автокодировщиком (автоэнкодером, PAE) (рис. 6б). Реализация с использованием ИНС (используется блок ЦОС на входе ИНС) стандартного предиктора исследуемого сигнала (рис. 5б) приведена на рис. 9. Реализация с использованием ИНС (используется блок ЦОС на входе ИНС) модифицированного прогнозирующего автоэнкодера (PAE) (рис. 6б) приведена на рис. 8.

На рис. 10 отображены две зависимости максимального количества прогнозируемых отсчётов сигнала (максимальной дальности прогноза), при условии не превышения ошибки прогноза заданной максимальной величины ошибки прогноза (среднеквадратичное отклонение (СКО) результата прогноза), от величины верхней частоты спектра прогнозируемого сигнала, для случаев использования стандартного предиктора (рис. 9) (пунктирная линия, рис. 10) и модифицированного прогнозирующего автокодировщика (автоэнкодера, PAE) (рис. 8) (чёрная линия, рис. 10), соответственно. Обучение ИНС производилось методом Левенберга-Марквардa на выборке сигнала длиной 5000 отсчетов, при этом распределение входных данных: подгонка – 70%, контроль – 15%, тестирование – 15%. Задаваемая максимальная величина ошибки прогноза на интервале тестирования соответствовала СКО=0.25. Верхняя частота спектра прогнозируемого сигнала формировалась фильтрацией исходного сигнала с использованием КИХ-ФНЧ с изменяемой частотой среза. На рис. 10 изменяемая частота среза КИХ-ФНЧ по оси абсцисс отображается в виде обратной величины – периода среза КИХ-ФНЧ, задаваемого в нормированных временных отсчётах.

На рис. 10 увеличение периода среза КИХ-ФНЧ по оси абсцисс соответствует уменьшению верхней частоты спектра прогнозируемого сигнала с выхода КИХ-ФНЧ, что повышает инерционность и увеличивает интервал автокорреляции прогнозируемого сигнала, соответственно, при этом увеличивается (как видно из рис. 10) дальность максимального прогноза при задаваемой фиксированной величине максимальной ошибки прогноза.

В результате сравнения, представленных на рис. 10 двух зависимостей дальности прогноза сигнала (при фиксированной ошибке прогноза сигнала) от верхней частоты спектра сигнала (пунктирная линия на рис. 10 – стандартный предиктор (рис. 9), чёрная линия на рис. 10 – модифицированный прогно-

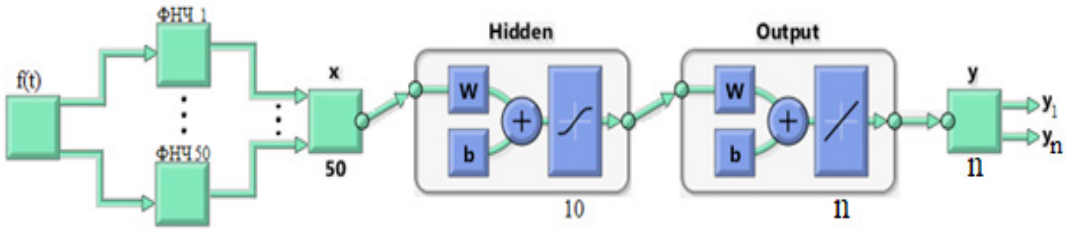

Рис. 9. Структурная схема прогнозирующего модуля: блок ЦОС и прогнозирующий блок с использованием ИНС

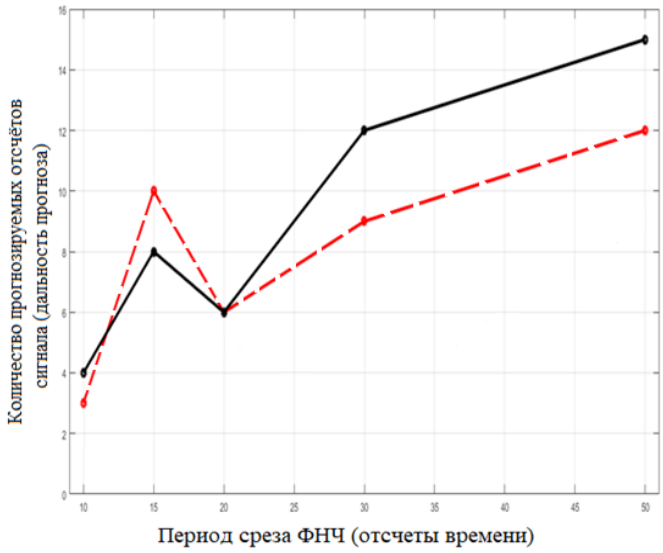

Рис. 10. Зависимость дальности прогноза сигнала от верхней частоты среза прогнозируемого сигнала

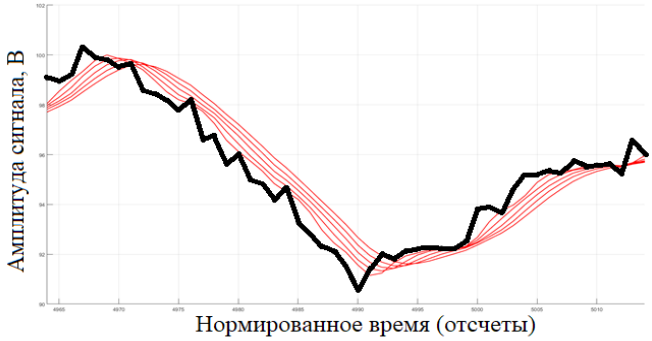

Рис. 11. Пять базовых компонент (тонкие линии) исходного сигнала (жирная чёрная линия), полученных с выходов гребёнки из пяти цифровых КИХ-ФНЧ

зирующий автокодировщик (автоэнкодер, PAE) (рис. 8)) следует вывод, что применение архитектуры PAE, то есть модификация прогнозирующего автокодировщика, представленная на рис.7 и реализованного в виде структуры, представленной на рис. 8, позволяет увеличить точность формируемого прогноза входного сигнала.

4. Формировании прогноза многокомпонентных временных рядов данных с использованием методов цифровой фильтрации и модифицированного прогнозирующего автокодировщика (автоэнкодера)

При формировании прогноза многокомпонентных временных рядов данных применяется технология ЦОС для разложения сложного многокомпонентного временного ряда на отдельные базовые компоненты (то есть, структурный анализ многокомпонентного временного ряда). Отфильтрованные базовые компоненты исходного сигнала формируются в результате прохождении сигнала через гребёнку цифровых ФНЧ и в получении на выходе набора отфильтрованных компонентов исходного сигнала. При таком подходе производится компонентное разложение исходного сигнала и последовательная фильтрация шумов с использованием параллельного набора цифровых ФНЧ.

На рис. 11 представлен результат структурного анализа многокомпонентного временного ряда, при этом исходный временной ряд данных (жирная чёрная линия, рис. 11) разложен на пять базовых компонент (тонкие линии, рис. 11), полученных с выходов гребенки из пяти цифровых КИХ-ФНЧ с периодами среза, равными величинам 7, 10, 13, 16, 19 отсчётов времени, соответственно. Период среза ФНЧ определяется как обратная величина частоты среза ФНЧ.

На рис. 12 представлен результат формирования архитектуры модульной ИНС для формирования прогноза в соответствии со структурой прогнозируемого многокомпонентного временного ряда. В данном примере на рис. 12 представлена архитектура мо-

дульной ИНС из пяти прогнозирующих модулей, представленных на рис. 8.

С использованием архитектуры модульной ИНС из пяти прогнозирующих модулей (рис. 8) и технологии «машинного обучения» для каждой из пяти базовых компонент исходного сигнала (рис. 11, тонкие линии), в соответствии с их динамическими характеристиками, формируются пять отдельных прогнозов с различным по длительности временным горизонтом.

На рис. 13 – 17 представлены сформированные пять отдельных прогнозов с различным по длительности временным горизонтом на 2, 3, 4, 5, 6 временных отсчётов вперед, для каждой из пяти базовых компонент (рис. 11, тонкие линии), соответственно. Также, на рис. 13 – 17 отображены доверительные интервалы (полосы) прогноза вперед для каждой из пяти базовых компонент, рассчитываемые в виде СКО каждой отфильтрованной базовой компоненты относительно исходного сигнала (рис. 11, жирная черная линия).

Более медленные и инерционные базовые компоненты (рис. 11, тонкие линии), до-

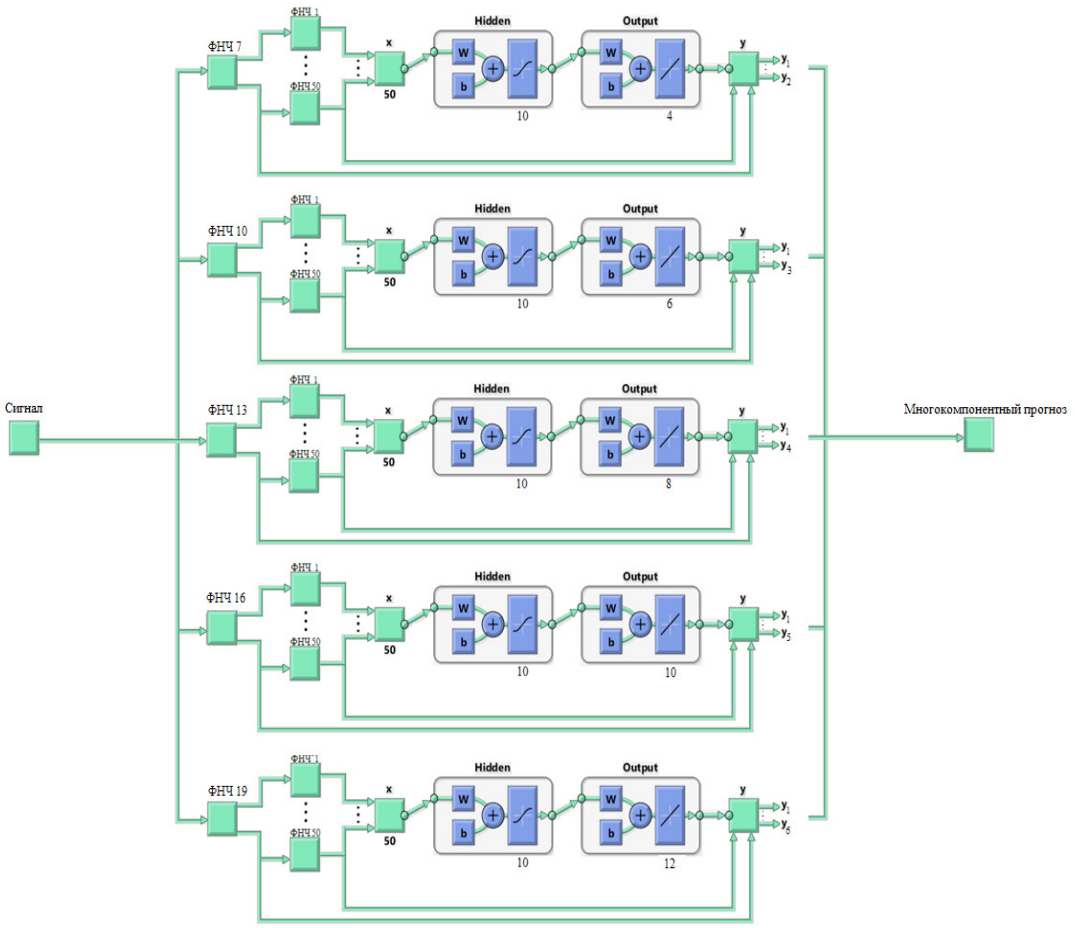

Рис. 12. Архитектуры модульной ИНС из пяти прогнозирующих модулей (рис. 8), формирующей многокомпонентный прогноз наблюдаемого временного ряда

пускают в результате более длительной автокорреляции, соответственно более длительный прогноз на больший интервал времени вперед, при этом доверительный интервал (полоса) прогноза каждой отфильтрованной базовой компоненты отражает прогнозное изменение исходного сигнала (рис. 11, жирная чёрная линия) в пределах доверительного интервала прогноза для каждой базовой компоненты (рис. 11, тонкие линии).

В таблице 1 приведены результаты расчета СКО ошибки прогноза (для каждой из пяти базовых компонент, рис. 11, тонкие линии) с различным по длительности временным горизонтом на 2, 3, 4, 5, 6 временных отсчётов вперед,

Далее, по полученным пяти отдельным прогнозам с различным временным горизонтом базовых компонент исходного сигнала (рис.18, жирная черная линия), формируется

Рис. 13. Результат прогнозирования первой компоненты с временным горизонтом на 2 отсчёта вперёд

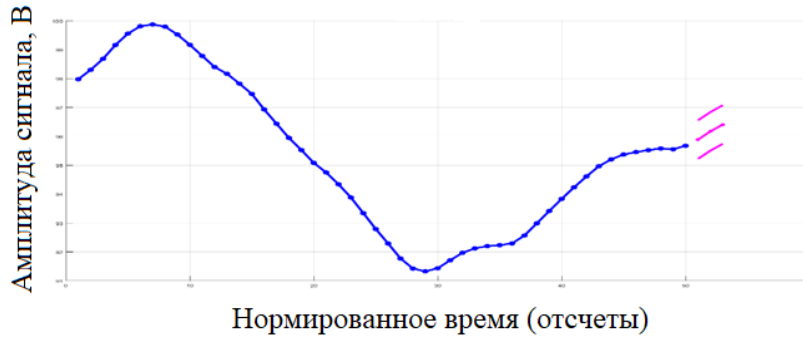

Рис. 14. Результат прогнозирования второй компоненты с временным горизонтом на 3 отсчёта вперёд

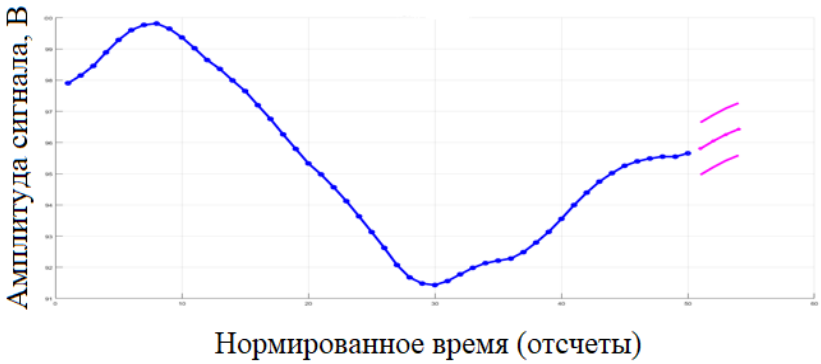

Рис. 15. Результат прогнозирования третьей компоненты с временным горизонтом на 4 отсчёта вперёд

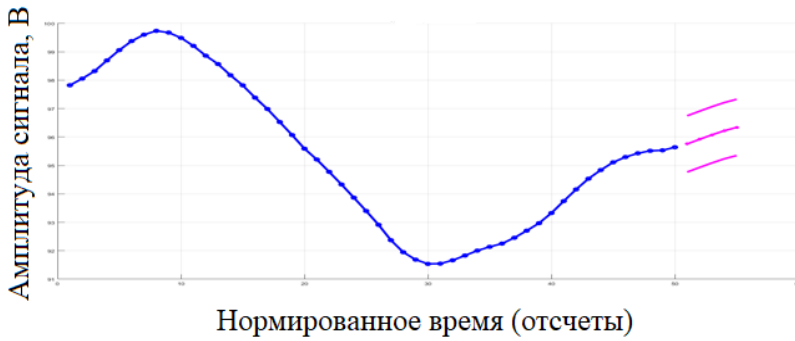

Рис. 16. Результат прогнозирования четвёртой компоненты с временным горизонтом на 5 отсчётов вперёд

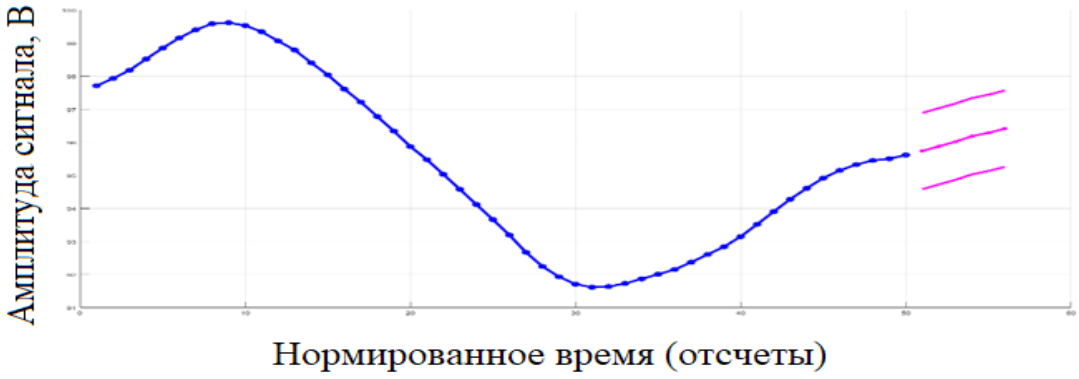

Рис. 17. Результат прогнозирования пятой компоненты с временным горизонтом на 6 отсчётов вперёд

Таблица 1

СКО сигналов на разных периодах среза ФНЧ

Период среза ФНЧ, (количество временных отсчётов).	Длительность временного горизонта, (количество временных отсчётов).	СКО
7	2	0,1777332
10	3	0,1898771
13	4	0,2009997
16	5	0,2156947
19	6	0,2249945

завершенный масштабируемый прогноз на различных временных интервалах (рис.18, тонкие линии).

Из отображенного результата прогноза (рис. 18, тонкие линии прогноза) следует, что самый ближний горизонт прогнозирования исходного многокомпонентного временного ряда (рис.18, жирная черная линия) определяется параметрами самой быстрой базовой компонентой (прогноз базовой компоненты, плюс доверительный интервал (полоса) прогноза базовой компоненты). Самый дальний горизонт прогнозирования исходного многокомпонентного временного ряда (рис.18, жирная черная линия) определяется самой медленной базовой компонентой и имеет максимальную ширину полосы прогноза (ширину доверительного интервала прогноза).

На рис. 19, более детально показан временной участок, соответствующий многоком-

Рис. 18. Сформированный прогноз исходного многокомпонентного временного ряда

понентному прогнозу (отображен на рис. 18, тонкие линии), также добавлен временной участок исходного прогнозируемого сигнала (рис. 18, жирная черная линия).

На рис. 19 отображено: сформированный многокомпонентный прогноз (пунктирные линии) исходного сигнала, добавлена жирная черная линия – продолжение исходного прогнозируемого сигнала на область сформированного многокомпонентного прогноза. Из рис. 19 следует, что сформированный многокомпонентный прогноз задает доверительную область прогноза исследуемого сигнала.

5. Заключение.

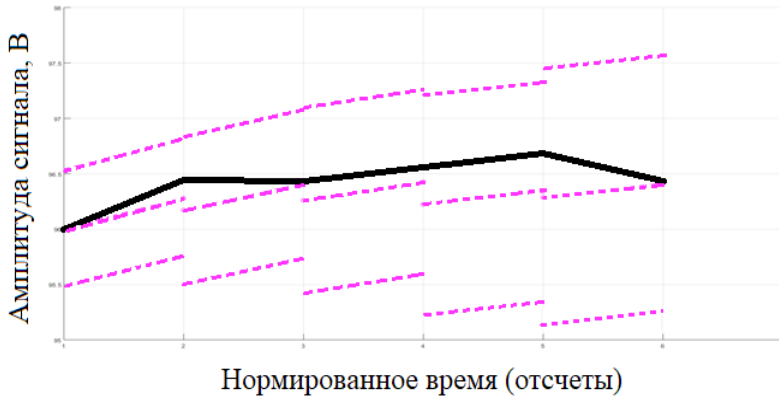

Рис. 19. Многокомпонентный прогноз (пунктирные линии) временного участка исходного сигнала (жирная чёрная линия)

Процессы, протекающие в АСУ ТП и отражаемые в наблюдаемых потоках данных, являются сложными многокомпонентными процессами, что существенно усложняет формирование их прогнозов. Для реализации многокомпонентного прогноза предлагается применять технологию ЦОС для разложения сложного многокомпонентного временного ряда на отдельные базовые компоненты (структурный анализ многокомпонентного временного ряда), также предлагается формировать модульную архитектуру ИНС для осуществления прогноза, в соответствии со структурой прогнозируемого многокомпонентного временного ряда.

При возникновении аномалий в работе АСУ ТП будут происходить структурные изменения в сигнале ошибки формируемого прогноза, в результате анализа этих структурных изменений ошибки прогноза, собственно происходит детектирование (обнаружение) аномалий в наблюдаемых процессах АСУ ТП. Предлагаемый подход формирования прогноза для каждой отдельной базовой компоненты прогнозируемого многокомпонентного временного ряда, в соответствии с их динамическими характеристиками, позволит обнаруживать в множестве наблюдаемых временных рядов данных АСУ ТП аномалии раздельно по их различным динамическим характеристикам, что повышает эффективность управления устойчивостью функционирования АСУ ТП в условиях воздействия кибератак.

При формировании многокомпонентного прогноза временных рядов данных АСУ ТП предлагается применять ИНС – модифицированный прогнозирующий автокодировщик (автоэнкодер, PAE). В проведённом исследовании показано, что ИНС – модифицированный прогнозирующий автокодировщик (автоэнкодер, PAE) позволяет увеличить точность формируемого прогноза входного сигнала, что важно при реализации обнаружения (детектирования) аномалий по результатам анализа структурных изменений, возникающих в сигнале ошибки формируемого прогноза исследуемого сигнала.

Литература

1. A. Ragozin, V.Telezhkin, P.Podkorytov, «Prediction of Aggregate Multicomponent Time Series in Industrial Automated Systems Using Neural Network», Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists 2019, 13-15 March, 2019, Hong Kong, pp. 17-19.

2. A. N. Ragozin, V. F. Telezhkin, P. S. Podkorytov. State Prediction in Control Systems via Compound Time Series: Neural Network Approach. EEE SoutheastCon 2019 Von Braun Center Huntsville, Alabama April 11th-14th, 2019. Pages 1–6.

3. A. N. Ragozin, V. F. Telezhkin, P. S. Podkorytov, «Forecasting Complex Multi-component Time Series within Systems Designed to Detect Anomalies in Dataflows of Industrial Automated Systems», SIN '19: Proceedings of the 12th International Conference on Security of Information and Networks, September 2019, Article No.: 2, pp. 1–5.

4. A. N. Sokolov, A. N. Ragozin, I. A. Pyatnitsky, S. K. Alabugin, «Applying of Digital Signal Processing Techniques to Improve the Performance of Machine Learning-based Cyber Attack Detection in Industrial

Control System», SIN '19: Proceedings of the 12th International Conference on Security of Information and Networks, September 2019, Article No.: 23, pp. 1–4.

5. Ragozin A. N. ; Osipov D. V. ; Tarasov I. S. ; Pletenkova A. D., Investigation of the Influence of the Preliminary Digital Filtering Method on the Accuracy of Sig-nal Prediction in Anomaly Detection Systems in Industrial Automatic Control Systems (IACS), 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT) 2020, 14-15 May, 2020, Yeka-terinburg, Russia,, pp. 1-4.

6. S. Tomonobu and T. Hitoshi, «One-hour-ahead load forecasting using neural network», IEEE Transactions on Power Systems, no. 1, pp. 21–24, 2002.

7. R. Huang, T. Huang, and Gadh, «Solar generation prediction using the ARMA model in a laboratory-level micro-grid», in IEEE Third International Conference on Smart Grid Communications, Sydney, 2012, pp. 528–533.

8. A. M. Abdurakhmanov, M. V. Volodin, E. Yu. Zybin, and V. N. Ryabchenko, «Methods for predicting power consumption in distribution networks (review)», Russian Internet Journal of Electrical Engineering, pp. 3–23, 2016.

9. A. N. Ragozin, A. A. Razumov, «Neural network forecasting with preliminary digital filtering of complex radio signals», in XVI International scientific and technicalconference Physics and technicalapplications of wave processes, Miass, 2018, pp. 285–290.

10. M. Granroth-Wilding and S. Clark, «What Happens Next? Event Prediction Using a Compositional Neural Network Model», AAAI, pp. 2727–2733, 2016.

11. Lee, R. M., Assante, M. J., & Conway, T. (2016). Analysis of the cyber attack on the Ukrainian power grid. SANS Industrial Control Systems, 23.

12. Xiao, Y. J., Xu, W. Y., Jia, Z. H., Ma, Z. R., & Qi, D. L. (2017). NIPAD: a non-invasive power-based anomaly detection scheme for programmable logic controllers. Frontiers of Information Technology & Electronic Engineering, 18(4), 519-534.

13. Wang, W., Xie, Y., Ren, L., Zhu, X., Chang, R., & Yin, Q. (2018, May). Detection of data injection attack in industrial control system using long short term memory recurrent neural network. In 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA) (pp. 2710-2715). IEEE.

14. Kravchik, M., & Shabtai, A. (2018, October). Detecting cyber attacks in industrial control systems using convolutional neural networks. In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy (pp. 72-83). ACM.

15. Muna, A. H., Moustafa, N., & Sitnikova, E. (2018). Identification of malicious activities in industrial internet of things based on deep learning models. Journal of Information Security and Applications, 41, 1-11

16. Potluri, S., Diedrich, C., & Sangala, G. K. R. (2017, September). Identifying false data injection attacks in industrial control systems using artificial neural networks. In 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA) (pp. 1-8). IEEE.

17. Yang, H., Chen, T., Guo, X., Wang, X., & Li, F. (2017, December). Research on intrusion detection of industrial control system based on OPSO-BPNN algorithm. In 2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC) (pp. 957-961). IEEE.

18. Demertzis, K., Iliadis, L., & Spartalis, S. (2017, August). A spiking one-class anomaly detection framework for cyber-security on industrial control systems. In International Conference on Engineering Applications of Neural Networks (pp. 122-134). Springer, Cham.

19. Wu, Z., Albalawi, F., Zhang, J., Zhang, Z., Durand, H., & Christofides, P. (2018). Detecting and Handling Cyber-attacks in Model Predictive Control of Chemical Processes. Mathematics, 6(10), 173.

20. Рагозин А.Н. Применение цифровой обработки сигналов и нейронной сети при формировании прогноза временных рядов данных для целей обнаружения аномалий при автоматизированном управлении технологическими процессами. Вестник УрФО. Безопасность в информационной сфере., No 1 (35), 2020. – С. 24–34.

References

1. A. Ragozin, V.Telezhkin, P.Podkorytov, «Prediction of Aggregate Multicomponent Time Series in Industrial Automated Systems Using Neural Network», Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists 2019, 13-15 March, 2019, Hong Kong, pp. 17-19.

2. A. N. Ragozin, V. F. Telezhkin, P. S. Podkorytov. State Prediction in Control Systems via Compound Time Series: Neural Network Approach. EEE SoutheastCon 2019 Von Braun Center Huntsville, Alabama April 11th-14th, 2019. Pages 1–6.

3. A. N. Ragozin, V. F. Telezhkin, P. S. Podkorytov, «Forecasting Complex Multi-component Time Series within Systems Designed to Detect Anomalies in Dataflows of Industrial Automated Systems», SIN '19:

Proceedings of the 12th International Conference on Security of Information and Networks, September 2019, Article No.: 2, pp. 1–5.

4. A. N. Sokolov, A. N. Ragozin, I. A. Pyatnitsky, S. K. Alabugin, «Applying of Digital Signal Processing Techniques to Improve the Performance of Machine Learning-based Cyber Attack Detection in Industrial Control System», SIN '19: Proceedings of the 12th International Conference on Security of Information and Networks, September 2019, Article No.: 23, pp. 1–4.

5. Ragozin A. N. ; Osipov D. V. ; Tarasov I. S. ; Pletenkova A. D., Investigation of the Influence of the Preliminary Digital Filtering Method on the Accuracy of Sig-nal Prediction in Anomaly Detection Systems in Industrial Automatic Control Systems (IACS), 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT) 2020, 14-15 May, 2020, Yeka-terinburg, Russia,, pp. 1-4.

6. S. Tomonobu and T. Hitoshi, «One-hour-ahead load forecasting using neural network», IEEE Transactions on Power Systems, no. 1, pp. 21–24, 2002.

7. R. Huang, T. Huang, and Gadh, «Solar generation prediction using the ARMA model in a laboratory-level micro-grid», in IEEE Third International Conference on Smart Grid Communications, Sydney, 2012, pp. 528–533.

8. A. M. Abdurakhmanov, M. V. Volodin, E. Yu. Zybin, and V. N. Ryabchenko, «Methods for predicting power consumption in distribution networks (review)», Russian Internet Journal of Electrical Engineering, pp. 3–23, 2016.

9. A. N. Ragozin, A. A. Razumov, «Neural network forecasting with preliminary digital filtering of complex radio signals», in XVI International scientific and technicalconference Physics and technicalapplications of wave processes, Miass, 2018, pp. 285–290.

10. M. Granroth-Wilding and S. Clark, «What Happens Next? Event Prediction Using a Compositional Neural Network Model», AAAI, pp. 2727–2733, 2016.

11. Lee, R. M., Assante, M. J., & Conway, T. (2016). Analysis of the cyber attack on the Ukrainian power grid. SANS Industrial Control Systems, 23.

12. Xiao, Y. J., Xu, W. Y., Jia, Z. H., Ma, Z. R., & Qi, D. L. (2017). NIPAD: a non-invasive power-based anomaly detection scheme for programmable logic controllers. Frontiers of Information Technology & Electronic Engineering, 18(4), 519-534.

13. Wang, W., Xie, Y., Ren, L., Zhu, X., Chang, R., & Yin, Q. (2018, May). Detection of data injection attack in industrial control system using long short term memory recurrent neural network. In 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA) (pp. 2710-2715). IEEE.

14. Kravchik, M., & Shabtai, A. (2018, October). Detecting cyber attacks in industrial control systems using convolutional neural networks. In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy (pp. 72-83). ACM.

15. Muna, A. H., Moustafa, N., & Sitnikova, E. (2018). Identification of malicious activities in industrial internet of things based on deep learning models. Journal of Information Security and Applications, 41, 1-11

16. Potluri, S., Diedrich, C., & Sangala, G. K. R. (2017, September). Identifying false data injection attacks in industrial control systems using artificial neural networks. In 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA) (pp. 1-8). IEEE.

17. Yang, H., Chen, T., Guo, X., Wang, X., & Li, F. (2017, December). Research on intrusion detection of industrial control system based on OPSO-BPNN algorithm. In 2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC) (pp. 957-961). IEEE.

18. Demertzis, K., Iliadis, L., & Spartalis, S. (2017, August). A spiking one-class anomaly detection framework for cyber-security on industrial control systems. In International Conference on Engineering Applications of Neural Networks (pp. 122-134). Springer, Cham.

19. Wu, Z., Albalawi, F., Zhang, J., Zhang, Z., Durand, H., & Christofides, P. (2018). Detecting and Handling Cyber-attacks in Model Predictive Control of Chemical Processes. Mathematics, 6(10), 173.

20. Ragozin A.N. Application of digital signal processing and neural network in the formation of time series prediction for the purpose of anomaly detection in automated process control. Bulletin of the Urals Federal District. Securityintheinformationfield, Vol 1 (35), 2020. – P. 24–34.

РАГОЗИН Андрей Николаевич, кандидат технических наук, доцент кафедры защиты информации, доцент кафедры инфокоммуникационных технологий высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: ragozinan@susu.ru

RAGOZIN Andrey, Candidate of Sciences in Technology, Department of Information Security, Department of Information Technology Federal State Autonomous Educational Institution of Higher Education «South Ural State University (national research university)» Russia, 454080, Chelyabinsk, prsp. Lenina, 76. E-mail: ragozinan@susu.ru

УДК 340.113 + 004.056 Вестник УрФО № 2(40) / 2021, с. 59–64

Жернова В.М.

DOI: 10.14529/secur210206

ПРЕДПОСЫЛКИ РАЗВИТИЯ ИНФОРМАЦИОННОГО ЗАКОНОДАТЕЛЬСТВА НА ПРИМЕРЕ КИБЕРФИЗИЧЕСКИХ СИСТЕМ[1]

В статье поднимается вопрос о соотношении объектов, развитие и использование которых, формируют новые элементы системы информационного права. К их числу относятся киберфизические системы, интернет вещей, искусственный интеллект и роботы. Законодательство относительно таких объектов развивается неравномерно, причем с упором на частные технологии, а не на систему в целом. В статье поднимается вопрос о необходимости усиления позиций нормотворчества относительно именно киберфизических систем, поскольку они включают различные возможные технологии и обладают возможностью формирования правоотношений относительно себя, но, в то же время, синергитически являются более мощным и важным объектом, нежели популярные на сегодняшний день роботы и искусственный интеллект. В исследовании приводится схема отношений множеств элементов интернета вещей, искусственного интеллекта, робототехники и киберфизических систем, что предполагает вывод о том, что объекты за исключением последнего, являются частными случаями для создания норм правового регулирования, а киберфизическим системам необходимо уделять большее внимание.

Ключевые слова: *киберфизические системы, интернет вещей, искусственный интеллект, роботы, правовой режим, информационное право, правоотношения, регулирование цифровых технологий, информация, большие данные, программное обеспечение, формирование правового режима, объект и предмет информационного права.*

[1] Исследование выполнено в рамках научного проекта РФФИ No 18-29-16014 «Место и роль правового регулирования в развитии цифровых технологий, правовое регулирование и саморегулирование, в том числе с учетом особенностей отраслей права»

Zhernova V.M.

PRECONDITIONS FOR THE DEVELOPMENT OF INFORMATION LEGISLATION ON THE EXAMPLE OF CYBER-PHYSICAL SYSTEMS

The study raises the question of the relationship between objects, the development and use of which forms new elements of the information law system. These include cyber-physical systems, the Internet of Things, artificial intelligence, and robots. Legislation regarding such objects is developing unevenly, with an emphasis on private technologies, and not on the system as a whole. The article raises the question of the need to strengthen the position of rule-making in relation to cyber-physical systems, since they include various possible technologies and have the ability to form legal relations with respect to themselves, but at the same time, synergistically, they are a more powerful and important object than robots and artificial intelligence which are more popular today. The study provides a diagram of the relationship between the sets of elements of the Internet of Things, artificial intelligence, robotics and cyber-physical systems, which suggests the conclusion that objects, with the exception of the latter, are special cases for creating legal regulation, and cyber-physical systems need to be given more attention.

Keywords: *cyber-physical systems, internet of things, artificial intelligence, robots, legal regime, information law, legal relations, regulation of digital technologies, information, big data, software, formation of a legal regime, object and subject of information law.*

Создание и использование киберфизических систем находится под воздействием норм различных отраслей права. Сложный, в физическом смысле, объект «киберфизические системы» представляет собой комплекс различных технологий, которые обеспечивают сбор, обработку и передачу информации, выполнение предписанных действий и т.д. С юридической точки зрения, киберфизические системы также представляют собой сложный объект, находящийся на стыке регулирования информационного права, авторского права, гражданского права, возможно в будущем, даже трудового права.

Вероятно, ввиду непонимания технической и юридической сложности этого объекта, ему уделяется крайне мало внимания в научной литературе и научных статьях, в крайнем случае – упоминание об отсутствии терминологии [1, с. 125] или же включением робототехники и искусственного интеллекта в состав киберфизической системы [2]. Причем, объекты робототехники также могут иметь в своем составе технологии искусственного интеллекта. В последние годы технологии и способы их использования задают тренд для формирования юридических норм по поводу новых, ранее не формированных, отношений, возникающих по поводу создания и использования таких технологий. К ним можно отнести технологию блокчейн и криптовалюту, технологию интернета вещей и киберфизические системы, технологию искусственного интеллекта и робототехнику и т.д.

В Распоряжении Правительства от 19 августа 2020 г. «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники на период до 2024 г.» (далее - Распоряжение) признается, что «отсутствие однозначного понимания содержания терминов «искусственный интеллект», «робот», «умный робот», «робототехника», «интеллектуальный агент» приводит к терминологиче-

ским проблемам при формировании регулирования».

Сложностям формирования дефениции «Киберфизическая система» посвящено несколько научных трудов. Так, например, Незнамов А.В. и Наумов В.Б.[2] говорят о том, что «точного определения этого термина нет…, при этом в одних источниках утверждается, что киберфизические системы интегрируют кибернетическое начало, компьютерные аппаратные и программные технологии, качественно новые исполнительные механизмы, встроенные в окружающую их среду и способные воспринимать ее изменения, реагировать на них, самообучаться и адаптироваться. В других подчеркивается, что ключевая идея таких систем — интеграция физического и информационного пространства».

Ученые отмечают, что на данный момент актуальна проблема отсутствия адекватного понимания уровня развития предметных общественных отношений и отсутствие междисциплинарных исследований, и проблема регулирования киберфизических систем недооценивается по той причине, что у регулятора часто отсутствует реальное понимание текущего уровня развития общественных отношений [2].

Таким образом, цель исследования – определить как соотносятся между собой новые объекты права, возможно, не всеми и не везде признанные: искусственный интеллект, киберфизические системы, интернет вещей и робототехника. Кроме того, авторы считают, что вопросам правового регулирования киберфизических систем следует уделять большее внимание, нежели сейчас представлено в научных исследованиях и на законодательном уровне, поскольку этот вопрос имеет большое значение для классификации новых правоотношений, что, в свою очередь, необходимо для определения структуры отдельных отраслей, отдельных правовых институтов.

Для формирования структуры соотношений, необходимо определить некоторые элементы правового режима, в которые, безусловно, нужно включить предмет и объект правоотношений в каждом случае.

На сегодняшний день нельзя отрицать тот факт, что формируется подотрасль права, регулирующая отношения по поводу цифровых технологий, куда можно с определенной уверенностью включить киберфизические системы и интернет вещей, искусственный интеллект и робототехнику. Первоначально, необходимо определить множества этих объектов, как они соотносятся друг с другом, и имеет место хотя бы частичное поглощение одной объекта другим. Предлагаем следующий вариант соотнесения исследуемых объектов, на основании существующих определений:

Согласно Указу Президента РФ от 10 октября 2019 г. «О развитии искусственного интеллекта в Российской Федерации», исскуственный интеллект - комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение, процессы и сервисы по обработке данных и поиску решений.

Интернет вещей является совокупностью сетей межмашинных коммуникаций и систем хранения/обработки больших данных, в которых за счет подключения датчиков и актуаторов (исполнительных механизмов) к сети реализуется цифровизация различных процессов и объектов. Такое определение представлено в Приказе Министерства цифрового развития, связи и массовых коммуникаций РФ от 29 марта 2019 г. «Об утверждении Концепции построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации».

Робот - программируемый исполнительный механизм с определенным уровнем автономности для выполнения перемещения, манипулирования или позиционирования, согласно определению 2018 ИСО/ТК 299 «Робототехника».

Киберфизические системы - это интеллектуальные системы, которые включают спроектированные взаимодействующие сети физических и вычислительных компонентов [3]. В таком определении к киберфизическим системам относятся и роботы, и беспилотный транспорт, и роботизированные устройства, что представляется вполне оправданным [2].

Так, на основании приведенных определений из документов различного уровня, мы приходим к выводу, что исследуемые понятия соотносятся следующим образом:

Рис. 1. Соотношение объектов

Стоит дать некоторые пояснения:

Интернет вещей и искусственный интеллект как технологии, безусловно, могут существовать отдельно, но тогда они не имеют смысла как часть объекта права. В отличие от интернета вещей киберфизическая система трактуется именно как система. Это обусловлено тем, что главным в ней являются технические устройства: исполнительные механизмы и распределённая система датчиков и приводов. Технологическая компонента остаётся вспомогательной [4, С. 20-22]. Роботы и киберфизические системы (КФС) с применением таких технологий становятся полноценными компонентами отношений, возникающих по поводу создания и использования этих самых объектов. Довольно сложно сформировать отношение между роботами и КФС, но, исходя из приведенных определений, можно выразить мысль, что множество КФС включает множество роботов, и как следствие, обладает всеми характеристиками и элементами правового режима, но не ограничиваясь. Примечательно, что создание рабочей группы Государственной Думы РФ по регулированию робототехники, искусственного интеллекта и киберфизических систем ставит эти три объекта фактически на один уровень.

Традиционно, предметом правового регулирования считается конкретный вид общественных отношений, регулируемых нормой определённой отрасли права. Если мы говорим об искусственном интеллекте, что в данном случае будет является объектом правоотношений, а что предметом? В общем и целом, искусственный интеллект без привязки к физической форме (физическим частям роботов и КФС) является программным обеспечением. Правовое регулирование программных средств в законодательстве Российской Федерации присутствует в уголовном кодексе, в административном, в гражданском, в зависимости от отношений, в которые вступает субъекты по поводу программного обеспечения.

Предметом для правоотношений в сфере ИВ являются отношения по поводу передачи информации.

На сегодняшний день в России присутствует полноценное законодательство в отношении информационных систем, где представлен упор на оборот информации, и логичным следствием является наличие отраслевого законодательства об обеспечении защиты персональных данных при их обработке в информационной системе, о защите государственной тайны при обработке в информационных системах и т.д. В этом плане предшественниками КФС можно считать встроенные системы реального времени, распределенные вычислительные системы, автоматизированные системы управления техническими процессами и объектами [4, С. 21], но с внедрением новых технологий, указанных выше.

Безусловно, законодательство относительно всех четырех сфер развивается как в России, так и за рубежом, но заметна тенденция активной разработки в сфере робототехники и ИИ, в сфере интернет вещей – создание многочисленных стандартов техническим комитетом 194 «Киберфизические системы», но разработки в сфере КФС не отличаются особой активностью.

Так, например, в Распоряжении подтверждается тезис о том, что в настоящее время в мире отсутствуют единые подходы к регулированию технологий искусственного

интеллекта и робототехники, что связано с наличием ряда проблем, не имеющих однозначного решения. Одно из концептуальных проблемных направлений регулирования можно определить как определение предмета и границ регулирования сферы использования систем искусственного интеллекта и робототехники.

Весьма вероятно, что в ближайшее будущее система информационного права пополнится новыми элементами, поскольку правовое регулирование в сфере цифровых технологий, а именно роботизированных и киберфизических систем будет сформировано. «Усложнение и появление новых общественных отношений в информационной сфере создают предпосылки для формирования таких новых институтов, как правовое регулирование искусственного интеллекта, блокчейна и иных распределенных систем, больших данных, цифровых финансовых активов, нейронных сетей и др.» [5, С. 83], несмотря на тот факт, что «в условиях отсутствия детальных исследований системы информационного права, к сожалению, в науке информационного права пока не сформировалась единая система» [6, С. 31].

Как отмечают исследователи, именно КФС стали причиной бурно роста интереса именно к обработке больших объемов данных в реальном времени [7, С. 48]. Законодательно предпринимаются попытки о регулировании отношений, возникающих по поводу больших данных, но источник их появления – киберфизические системы – не находит должного регулирования на законодательном уровне.

Таким образом, на основании приведенной схемы отношений множеств интернета вещей, искусственного интеллекта, киберфизических систем и роботов и данных пояснений, считаем необходимым формировать правовые нормы не только в отношении искусственного интеллекта и роботов, но и первостепенно в отношении КФС, поскольку данный объект включает все указанные сущности и их совместная работа порождает новые отношения, ранее не определенные, а, соответственно, не находящие должного правового регулирования.

Литература

1. В.Ф. Изотова. Проблемы правового регулирования искусственного интеллекта киберфизических систем и робототехники. Проблемы и вызовы цифрового общества: тенденции развития правового регулирования цифровых трансформаций. Сборник научных трудов по материалам I международной научно-практической конференции под редакцией Н.Н. Ковалевой. 2019 С. 125-127.

2. А.В. Незнамов, В.Б. Наумов. Стратегия регулирования робототехники и киберфизических систем. Электронный доступ URL : https://zakon.ru/magazine/zakon/496 (дата обращения 11.03.2021)

3. Национальный институт стандартов и технологий США. CPS Framework Release 1.0 Электронный доступ. URL http:// pages.nist.gov/cpspwg/ (дата доступа 23.03.2021).

4. Куприяновский В.П., Намиот Д.Е., Синягов С.А. Киберфизические системы как основа цифровой экономики. International Journal of Open Information Technologies. 2016. №2. С.18-24.

5. Полякова Т. А., Минбалеев А. В., Кроткова Н. В. Формирование системы информационного права как научного направления: этапы развития и перспективы. Государство и право. 2019. №2 .С. 80-92.

6. Минбалеев А. В. Подотрасль права как правовой феномен (на примере права массовых коммуникаций) Вестник ЮУрГУ. Серия «Право». 2013. № 4. С. 28-32.

7. Namiot D. On Big Data Stream Processing //International Journal of Open Information Technologies. 2015. № 8. С. 48-51.

References

1. V.F. Izotov. Problems of legal regulation of artificial intelligence of cyber-physical systems and robotics. Problems and challenges of a digital society: trends in the development of legal regulation of digital transformations. Collection of scientific papers based on the materials of the 1st international scientific-practical conference edited by N.N. Kovaleva. 2019 Pp. 125-127. (in Russian)

2. A.V. Neznamov, V.B. Naumov. A strategy for regulating robotics and cyber-physical systems. Electronic access URL: https://zakon.ru/magazine/zakon/496 (date of treatment 03/11/2021) (in Russian)

3. US National Institute of Standards and Technology. CPS Framework Release 1.0 Electronic Access. URL http: // pages.nist.gov/cpspwg/ (accessed 03/23/2021).

4. Kupriyanovskiy V.P., Namiot D.E., Sinyagov S.A. Cyber-physical systems as the basis of the digital economy. International Journal of Open Information Technologies. 2016. №. 2. Pp.18-24. (in Russian)

5. Polyakova T. A., Minbaleev A. V., Krotkova N. V. Formation of the information law system as a scientific direction: stages of development and prospects. State and law. 2019. №. 2. Pp 80-92. (in Russian)

6. Minbaleev A. V. Sub-branch of law as a legal phenomenon (by the example of the law of mass communications) Vestnik SUSU. Series "Right". 2013. №. 4. Pp. 28-32. (in Russian)

7. Namiot D. On Big Data Stream Processing // International Journal of Open Information Technologies. 2015. №. 8. Pp. 48-51.

ЖЕРНОВА Влада Михайловна, кандидат юридических наук, доцент кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: zhernovavm@susu.ru

ZHERNOVA Vlada, Ph.D. in law, Associate Professor of the Department of Information Security, South Ural State University (National Research University). 454080, Chelyabinsk, etc. them. IN AND. Lenin, 76. E-mail: zhernovavm@susu.ru

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

УДК 340.113 + 004.056

Вестник УрФО № 2(40) / 2021, с. 65–71

Минбалеев А.В.

DOI: 10.14529/secur210207

ПРОБЛЕМЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ПРИ РАСПРОСТРАНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ В СЕТИ ИНТЕРНЕТ ПО ОБНОВЛЕННОМУ ЗАКОНОДАТЕЛЬСТВУ[1]

С принятием в России Федерального закона от 30.12.2020 № 519-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» введены новые требования в части распространения персональных данных. Для распространения персональных данных и последующей обработки персональных данных, разрешенных субъектом персональных данных для распространения нужно отдельное согласие. Таким образом, на оператора персональных данных налагаются дополнительные обязанности по получению согласия субъекта на произведение действий, направленных на распространение. Введенные требования не отменяют обязанности по получению согласия субъекта персональных данных на их обработку. На практике новые требования вызывают ряд вопросов, особенно в части распространения персональных данных в сети Интернет, а также в связи с необходимостью принятия мер по обеспечения кибербезопасности в части защиты прав субъектов персональных данных. В статье содержатся комментарии к новеллам законодательства и рекомендации операторам по обеспечению кибербезопасности персональных данных.

Ключевые слова: *кибербезопасность, информационная безопасность, правовое регулирование, персональные данные, распространение персональных данных в сети Интернет.*

[1] Работа выполнена при финансовой поддержке Совета по грантам Президента Российской Федерации (грант МД-2209.2020.6) «Развитие системы правовых средств обеспечения кибербезопасности в Российской Федерации».

Minbaleev A.V.

PROBLEMS OF LEGAL PROVISION OF CYBERSECURITY IN THE DISSEMINATION OF PERSONAL DATA ON THE INTERNET UNDER THE UPDATED LEGISLATION

With the adoption in Russia of Federal Law No. 519-FZ of 30.12.2020 "On Amendments to the Federal Law "On Personal Data", new requirements regarding the dissemination of personal data have been introduced. For the dissemination of personal data and the subsequent processing of personal data authorized by the subject of personal data for dissemination, a separate consent is required. Thus, the operator of personal data is subject to additional obligations to obtain the consent of the subject to perform actions aimed at dissemination. The introduced requirements do not cancel the obligation to obtain the consent of the subject of personal data for their processing. In practice, the new requirements raise a number of questions, especially in terms of the dissemination of personal data on the Internet, as well as in connection with the need to take measures to ensure cybersecurity in terms of protecting the rights of personal data subjects. The article contains comments on new legislation and recommendations to operators on ensuring the cybersecurity of personal data.

Keywords: *cybersecurity, information security, legal regulation, personal data, distribution of personal data on the Internet.*

Федеральный закон от 30.12.2020 № 519-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» [1] ввел новый правовой режим именно для персональных данных, разрешенных субъектом персональных данных для распространения. Для распространения персональных данных и последующей обработки персональных данных, разрешенных субъектом персональных данных для распространения нужно отдельное согласие (ст.10.1 Федерального закона «О персональных данных» [2] (далее – Закон). Данная статья накладывает на оператора дополнительные обязательства по получению согласия субъекта на произведение действий, направленных на распространение и не отменяет обязанностей по получению согласия субъекта персональных данных на их обработку (Согласие на «иную обработку» (кроме распространения) должно быть получено по общим правилам получения согласия статьи 9 Закона (в случае отсутствия иных оснований для обработки п. 2-9.1, 11 ч. 1 ст.6 Закона).

В иных случаях следует руководствоваться нормами ч. 1 ст. 6 Закона – т.е. либо согласие (п. 1 ч. 1 ст. 6 Закона), либо иные основания (п. 2-9.1, 11 ч. 1 ст. 6 Закона). Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения (далее – «согласие на распространение»), должно быть оформлено отдельно от иных согласий субъекта персональных данных. Оператор обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на распространение. Молчание или бездействие гражданина ни при каких обстоятельствах не может

считаться согласием. Согласие на распространение может быть предоставлено оператору непосредственно или с использованием специальной информационной системы Роскомнадзора.

Согласие должно быть получено отдельно при любой передаче персональных данных третьим лицам. Термин «передача персональных данных», согласно п. 3 ст. 3 Закона, включает в себя распространение, предоставление, доступ. Понятие «доступ» входит в «передачу персональных данных» как отдельное действие. Согласно п. 3 ст. 3 Закона «использование» является лишь одним из действий/операций, совершаемыми с персональными данными в рамках обработки и требует получения согласия, в том числе в рамках согласия на обработку. Соответственно, согласие на доступ и использование должны быть оформлены отдельно от согласия на распространение. Можно оформить соответствующие согласия и в рамках общего согласия на обработку персональных данных.

Ранее операторы зачастую оформляли право распространять персональные данные, просто включив в текст общего согласия на обработку персональных данных слово «распространение» при указании перечня действий с персональными данными, на которые дается согласие, или сделав отсылку к п. 3 ст. 3 Федерального закона «О персональных данных», который содержит определение «обработки персональных данных», или указав, что согласие дается на любые не запрещенные законом действия с персональными данными. Теперь формулировки согласия должны прямо и недвусмысленно разрешать распространение персональных данных, при этом должен быть указан четкий перечень персональных данных, в отношении которых разрешено распространение. Неоднозначные и неясные формулировки будут трактоваться в пользу субъекта персональных данных, оператор будет иметь возможность осуществлять только обработку (при наличии согласия на нее), но не распространение.

В согласии на распространение могут быть установлены запреты на передачу (кроме предоставления доступа) персональных данных оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) персональных данных неограниченным кругом лиц. Это означает, в частности, что пользователи социальных сетей и иных Интернет-ресурсов, позволяющих пользователям делиться информацией с неограниченным кругом лиц, смогут установить запрет на обработку опубликованных ими персональных данных неограниченным кругом лиц или в определенных целях.

Установленные субъектом запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) распространяемых персональных данных не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством РФ.

При отсутствии таких запретов дополнительного согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения не нужно.

В настоящее время принят приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения» (Зарегистрировано в Минюсте России 21.04.2021 № 63204), вступающий в силу с 1 сентября 2021 г. [3] Из содержания приказа также следует, что согласие на распространение оформляется отдельно от других согласий.

На практике сегодня возникает вопрос, учитывая положения пп. 9 и 10 ст. 10.1 Закона, о том, коррелируют ли термины п. 9 «запреты на передачу (кроме предоставления доступа) этих персональных данных оператором неограниченному кругу лиц» и «запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц» с терминами п. 10 «условиях обработки» и «запреты и условия на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения» соответственно?

Общая расшифровка термина «условия обработки» приведена в ст. 6 Закона. Представляется, что ч. 9 ст. 10.1 Закона не противоречит общему понятию «условий обработки», установленному в ст. 6 Закона. Ст. 10.1 Закона устанавливаются особенности содержания от-

дельного согласия субъекта персональных данных, получаемого в отношении данных, разрешенных для распространения, предусматриваются дополнительные возможности физических лиц по осуществлению контроля над обработкой персональных данных, в отношении которых было предоставлено согласие на их распространение, в частности предусматривается возможность наложения дополнительного запрета обработки персональных данных неограниченным кругом лиц [2].

Таким образом, термин «условия обработки», используемый частью 10 ст. 10.1 Закона, полностью коррелирует с термином «условия обработки», используемым ст. 6 названного Федерального закона и дополняется в соответствии с ч. 9 ст. 10.1 только в отношении категории «персональных данных, разрешенных субъектом персональных данных для распространения».

Все условия и запреты, предусмотренные п. 9 ст. 10.1 Закона, должны быть опубликованы в рамках указанной информации об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения, предусмотренной п. 10 ст. 10.1. Закона.

Термин «условия обработки» по большей части сводится к публикации сведений о правовом основании обработки (пп.1-11 ч.1 ст.6 Закона), если не затрагиваются персональные данные специальных категорий и биометрические персональные данные, и отсутствует поручение обработки. В случае же распространения персональных данных на ресурсах, где происходит распространение, должна быть информация об условиях обработки в части распространения (соответственно указание на наличие согласия, оформленного в соответствии со ст. 10.1 Закона), а также запреты (например, запрет на распространение каких-то конкретных сведений о лице, запрет на распространение через определенные сайты и т.п.) и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения (например, может быть указана необходимость оператора уведомлять субъекта персональных данных через какой сайт происходит распространение его персональных данных).

Возникает и вопрос, на каком ресурсе оператор обязан опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения?

Оператор обязан в срок не позднее трех рабочих дней с момента получения соответствующего согласия субъекта персональных данных опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения. Этот пункт вступит в силу с 01 июля 2021 года.

В настоящее время указанный ресурс однозначно законодательно не определен. Исходя из системного толкования Закона, таким ресурсом должен быть ресурс, на котором указанные персональные данные распространяются. Полагаем, если персональные данные распространяются неограниченному кругу лиц оператором на нескольких ресурсах, то информация (выполнение требований п. 10 ст. 10.1 Закона) должна размещаться на каждом ресурсе, например, сайтах в сети «Интернет». Причем распространять эту информацию необходимо на странице сайта в сети «Интернет», где эта информация распространяется.

С учетом того, что действия, направленные на распространение персональных данных, входят в общее понятие «обработки» персональных данных и не являются новым элементом законодательства, при публикации условий обработки также следует руководствоваться правилами, ранее установленными законодательством.

Таким образом, публикация условий обработки персональных данных в отношении категории «персональных данных, разрешенных субъектом персональных данных для распространения» определяется общим правилом, установленным ч. 2 ст. 18.1 Закона и не подразумевает создания отдельных ресурсов для публикации дополнительных условий.

Ч. 2 ст. 18.1 Закона установлено, что оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных [2]. Оператор, осуществляющий сбор персональных данных

с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

Пока условия для распространения информации не вступили в силу, системное толкование норм Закона свидетельствует, что запреты на передачу (кроме предоставления доступа) этих персональных данных оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц, должны быть установлены в документе, определяющем политику оператора в отношении обработки персональных данных, сведения о реализуемых требованиях к защите персональных данных. Также рекомендуется размещать их на страницах сайтов, на которых происходит распространение персональных данных неограниченному кругу лиц.

Возникает часто и вопрос о форме согласия на распространение. Представляется, что к такому согласию (в части его формы) полностью применяются требования ч. 4 ст. 9 Закона. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с Федеральным законом «Об электронной подписи». Во втором случае заверить его работник должен своей электронной подписью (ч. 1, 4 ст. 9 Закона).

По новым правилам оформлять письменное согласие необходимо, если вы собираетесь размещать информацию о сотруднике в открытом доступе (например, в социальных сетях, на доске почёта или на сайте организации) или передавать третьим лицам: охранным организациям, кадровым агентствам, аудиторским компаниям и т.д. Ранее согласие сотрудника не требовалось на перепечатку той информации, которую он сам разместил в сети «Интернет» или в других публичных ресурсах (п. 10 ч. 1 ст. 6 Закона). Данный пункт Закона утратил силу с 1 марта 2021 г. в силу Федерального закона от 30.12.2020 № 519-ФЗ.

Также необходимо отметить, что при установлении требований к согласию необходимо различать требования к форме и содержанию. Применительно к форме согласия на распространение персональных данных (например, публикация персональных данных работников в сети Интернет, которая также является распространением) – его необходимо получать по общим правилам получения согласий, установленным в части 4 статьи 9 Закона.

Применительно к содержанию согласия – с 01.03.2021 такое согласие может быть получено по новым правилам (то есть по правилам статьи 10.1 и в соответствии с формой, установленной ч. 9 ст. 9 Закона). Ч. 9 ст. 9 прямо предусматривает, что требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, устанавливаются уполномоченным органом по защите прав субъектов персональных данных. Пока такой акт не принят, применительно к согласию на распространение необходимо руководствоваться требованиями к содержанию, установленные ст. 10.1 Закона.

В соответствии с изменениями, внесенными в законодательство о защите персональных данных с 01 марта 2021 года, общие правила получения письменного согласия субъекта персональных данных (в том числе работника) на обработку дополняются требованиями к получению отдельного письменного согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, при этом работнику нужно дать возможность определить их перечень по каждой категории, указанной в согласии на обработку.

Также надо учитывать, что в соответствии с частью 9 статьи 9 Федерального закона «О персональных данных» требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, устанавливаются уполномоченным органом по защите прав субъектов персональных данных (Роскомнадзор) [4-6].

Согласно приказу Роскомнадзора от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку

персональных данных, разрешенных субъектом персональных данных для распространения» установлен ряд таких требований [3].

Также надо учитывать, что согласно п. 4 ст. 7 Федерального закона от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» «для обработки органами, предоставляющими государственные услуги, органами, предоставляющими муниципальные услуги, иными государственными органами, органами местного самоуправления, подведомственными государственным органам или органам местного самоуправления организациями, участвующими в предоставлении предусмотренных частью 1 статьи 1 настоящего Федерального закона государственных и муниципальных услуг, персональных данных в целях предоставления персональных данных заявителя, имеющихся в распоряжении таких органов или организаций, в орган, предоставляющий государственную услугу, орган, предоставляющий муниципальную услугу, либо подведомственную государственному органу или органу местного самоуправления организацию, участвующую в предоставлении предусмотренных частью 1 статьи 1 настоящего Федерального закона государственных и муниципальных услуг, либо многофункциональный центр на основании межведомственных запросов таких органов или организаций для предоставления государственной или муниципальной услуги по запросу о предоставлении государственной или муниципальной услуги, а также для обработки персональных данных при исполнении многофункциональным центром функций в соответствии со статьей 16 настоящего Федерального закона и при регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг и на региональных порталах государственных и муниципальных услуг не требуется получение согласия заявителя как субъекта персональных данных в соответствии с требованиями статьи 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» [7].

Анализ изменений законодательства о персональных данных свидетельствует о серьезном ужесточении требований в части распространения персональных данных неограниченному кругу лиц, в том числе через сеть Интернет. Изменения, внесенные в Закон, отличаются неоднозначностью формулировок и вызывают массу споров на практике. Полагаем, что толкование норм ст. 10.1 Закона должна происходить из позиции приоритета интересов субъектов персональных данных. В то же время Закон позволяет в определенных случаях субъектам персональных данных в определенной мере злоупотреблять своими правами. Так, сегодня часто субъекты в согласиях специально указывают, что они определяться позднее с условиями распространения, ставят распространение под те или иные условия. Делается это преднамеренно, с целью дальнейшего оспаривания распространения и требования через суд компенсации морального вреда в связи с незаконной обработкой персональных данных. Многие операторы при этом полагают, что если субъект подписал согласие на распространение, то этого достаточно. Однако, нормы ст. 10.1 Закона четко определяют необходимость максимальной конкретизации позиции субъекта. В связи с этим операторам сегодня важно чрезвычайно внимательно изучать полученные согласия и принимать оперативные меры по уточнению согласий или прекращению распространения персональных данных.

Литература

1. Федеральный закон от 30.12.2020 № 519-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» // Собрание законодательства РФ. 2021. № 1 (часть I). Ст. 58.

2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3451.

3. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 21.04.2021.

4. Брызгин, А. А. Правовой режим биометрических персональных данных / А. А. Брызгин, А. В. Минбалеев // Вестник УрФО. Безопасность в информационной сфере. – 2012. – № 2(4). – С. 35-41.

5. Минбалеев, А. В. Проблемы защиты персональных данных и цифрового профиля человека в

сети интернет в условиях пандемии / А. В. Минбалеев, В. А. Филоненкова // Вестник Южно-Уральского государственного университета. Серия: Право. – 2020. – Т. 20. – № 3. – С. 89-94.

6. Захаров, М. Н. Правовая защита персональных данных / М. Н. Захаров, А. В. Минбалеев // Безопасность информационного пространства : сборник трудов XIII Всероссийской научно-практической конференции студентов, аспирантов и молодых учёных, Челябинск, 26–28 ноября 2014 года / Министерство образования и науки Российской Федерации, Южно-Уральский государственный университет, Кафедра «Безопасность информационных систем». – Челябинск: Издательский центр ЮУрГУ, 2015. – С. 211-215.

7. Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // Собрание законодательства РФ. 2010. № 31. Ст. 4179.

References

1. Federal'nyj zakon ot 30.12.2020 № 519-FZ «O vnesenii izmenenij v Federal'nyj zakon «O personal'nyh dannyh» // Sobranie zakonodatel'stva RF. 2021. № 1 (chast' I). St. 58.

2. Federal'nyj zakon ot 27.07.2006 № 152-FZ «O personal'nyh dannyh» // Sobranie zakonodatel'stva RF. 2006. № 31 (1 ch.). St. 3451.

3. Prikaz Federal'noj sluzhby po nadzoru v sfere svyazi, informacionnyh tekhnologij i massovyh kommunikacij ot 24.02.2021 № 18 «Ob utverzhdenii trebovanij k soderzhaniyu soglasiya na obrabotku personal'nyh dannyh, razreshennyh sub"ektom personal'nyh dannyh dlya rasprostraneniya» // Oficial'nyj internet-portal pravovoj informacii http://pravo.gov.ru, 21.04.2021.

4. Bryzgin, A. A. Pravovoj rezhim biometricheskih personal'nyh dannyh / A. A. Bryzgin, A. V. Minbaleev // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. – 2012. – № 2(4). – S. 35-41.

5. Minbaleev, A. V. Problemy zashchity personal'nyh dannyh i cifrovogo profilya cheloveka v seti internet v usloviyah pandemii / A. V. Minbaleev, V. A. Filonenkova // Vestnik YUzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Pravo. – 2020. – T. 20. – № 3. – S. 89-94.

6. Zaharov, M. N. Pravovaya zashchita personal'nyh dannyh / M. N. Zaharov, A. V. Minbaleev // Bezopasnost' informacionnogo prostranstva : sbornik trudov XIII Vserossijskoj nauchno-prakticheskoj konferencii studentov, aspirantov i molodyh uchyonyh, CHelyabinsk, 26–28 noyabrya 2014 goda / Ministerstvo obrazovaniya i nauki Rossijskoj Federacii, YUzhno-Ural'skij gosudarstvennyj universitet, Kafedra «Bezopasnost' informacionnyh sistem». – CHelyabinsk: Izdatel'skij centr YUUrGU, 2015. – S. 211-215.

7. Federal'nyj zakon ot 27.07.2010 № 210-FZ «Ob organizacii predostavleniya gosudarstvennyh i municipal'nyh uslug» // Sobranie zakonodatel'stva RF. 2010. № 31. St. 4179.

МИНБАЛЕЕВ Алексей Владимирович, доктор юридических наук, профессор, зав. кафедрой информационного права и цифровых технологий, Московский государственный юридический университет имени О. Е. Кутафина (МГЮА); профессор кафедры теории государства и права, конституционного и административного права, Южно-Уральский государственный университет. 454080, г. Челябинск, пр. Ленина, 76, alexmin@bk.ru.

MINBALEEV Aleksey, Doctor of Sciences (Law), Professor, head Department of Information Law and Digital Technologies of Kutafin Moscow State Law University (MSAL); Professor of the Department of Theory of State and Law, Constitutional and Administrative Law, South Ural State University. 76 Lenin Ave., Chelyabinsk, 454080, alexmin@bk.ru.

Материалы к публикации отправлять по адресу E-mail: urvest@mail.ru
в редакцию журнала «Вестник УрФО. Безопасность в информационной сфере».

Или по почте по адресу: Россия, 454080, г. Челябинск, пр. им. Ленина, д. 76,
ЮУрГУ, Издательский центр.

ВЕСТНИК УрФО
Безопасность в информационной сфере № 2(40) / 2021
Подписано в печать 30.06.2021.
Дата выхода в свет 12.07.2021. Формат 70×108 1/16. Печать цифровая.
Усл.-печ. л. 6.3. Тираж 100 экз. Заказ 213/248.
Цена свободная.

Отпечатано в типографии Издательского центра ЮУрГУ.
454080, г. Челябинск, пр. им. В. И. Ленина, 76.

Bulletin of the Ural Federal District
Security in the Sphere of Information No. 2(40) / 2021
Signed to print June 30, 2021.
Date of publication of the 12.07.2021. Format 70×108 1/16. Screen printing.
Conventional printed sheet 6.3. Circulation – 100 issues. Order 213/248. Open price.

Printed in the printing house of the Publishing Center of SUSU.
76, Lenina Str., Chelyabinsk, 454080