Literatura

1. *Alad'ev V.Z.* Komp'yuternaya khrestomatiya. Spravochnoe rukovodstvo. Rabota zhestkogo diska. M.: Rossijskaya entsiklopediya, 2012. 337s.
2. *Arkhipenkov S.Ya., Golubev D.V., Maksimenko O.B.* Khranilishcha dannykh. M.: Dialog-MIFI, 2002. 528 c.
3. *Barsegyan A.A. i dr.* Metody i modeli analiza dannykh OLAP i Data Mining. Gl. 4–5, 7. SPb.: BKhV-Peterburg, 2004.
4. Vychislitel'nyj kompleks "Sivuch-1". Rukovodstvo po ekspluatatsii. TVGI. 466535. 130-01 RE. M.: MTsST, 2014. 124 s.
5. *Golubev D., Lobanov A.* Seti khraneniya dannykh (SAN) // Jet Info. 2002. № 9. C. 2–16.
6. *Zakharov A.I., Bryakalov G.A., Mikhajlova P.I., Chumakova E.V.* Metodika rascheta i otsenki sostava IT-oborudovaniya tsentra obrabotki dannykh // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2019. Vyp. 2. S. 31–40.
7. *Zakharov A.I., Bryakalov G.A., Chmykhova Ya.V.* Metodika otsenki vozmozhnostej vychislitel'nykh sredstv tsentra obrabotki dannykh // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2019. Vyp. 1. S. 124–129.
8. *Kim A.K. i dr.* Mikroprotsessory i vychislitel'nye kompleksy semejstva "El'brus": uchebnoe posobie. SPb.: Piter, 2013. 272 s.
9. *Ushakov N.N.* Tekhnologiya elementov vychislitel'nykh mashin. Struktury khraneniya informatsii. M.: Vysshaya shkola, 2001. 413 c.
10. SATA i drugie interfejsy zhestkikh diskov // ITC.ua. URL: http://itc.ua/articles/sata_i_drugie_interfejsy_zhestkih_diskov_22528 (data obrashcheniya: 08.07.2020).

DOI: 10.25586/RNU.V9187.20.03.P.090 УДК 123.2

В.А. Максимов, А.В. Калюжный, В.Е. Салимоненко

АЛГОРИТМ СИММЕТРИЧНОГО ШИФРОВАНИЯ ДЛЯ ПРОГРАММНОГО КОМПЛЕКСА ЗАЩИЩЕННОГО ОБМЕНА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Представлен оригинальный алгоритм симметричного шифрования, а также описан программный комплекс информационного обмена, использующий данный алгоритм. Отличительными особенностями алгоритма являются невысокая вычислительная сложность и малая информационная избыточность, вносимая в исходные открытые данные. Программный комплекс может быть использован в автоматизированных системах специального назначения либо в других системах, где требуется защищенный обмен информацией.

Ключевые слова: шифрование, алгоритм, защита информации.

V.A. Maksimov, A.V. Kalyuzhnyj, V.E. Salimonenko

SYMMETRIC ENCRYPTION ALGORITHM FOR THE SOFTWARE PACKAGE SECURE INFORMATION EXCHANGE IN AUTOMATED SYSTEMS

The article presents an original algorithm for symmetric encryption, as well as describes a software package for information exchange that uses algorithm. The distinctive features of the algorithm are low computational complexity and low information redundancy introduced into the source open data. The software package can be used in special automated systems or in other systems where secure information exchange is required.

Keywords: encryption, algorithm, information protection.

Введение

В современном мире все больше и больше возрастает значимость информации [1]. А в таких областях, как обороноспособность страны, защита национальных интересов, вопросы обеспечения конфиденциальности являются первоочередной задачей [7] на любом этапе обработки данных. Для успешного выполнения этой задачи применяются всевозможные методы [9] и способы защиты информации [2], и одним из таковых является ее шифрование.

С технологическими прорывами в области электроники появляются новые образцы информационно-вычислительных систем и сетей [3], имеющие большую производительность в сравнении со своими предшественниками, способные выполнять бóльшее количество операций за такт. Это позволяет в сравнительно короткие сроки проводить анализ существующих алгоритмов преобразования данных [4] и на основе выявленных уязвимостей выполнять вскрытие зашифрованной информации.

Для увеличения конфиденциальности сведений ограниченного доступа разработан программный комплекс защищенного обмена информацией на основе оригинального алгоритма шифрования.

Описание оригинального алгоритма шифрования

Вся информация, хранящаяся на цифровых носителях, представлена в виде массива логических «единиц» и «нулей». В совокупности эти «цифры» образуют числа в двоичной системе счисления (далее – СС) (рис. 1).

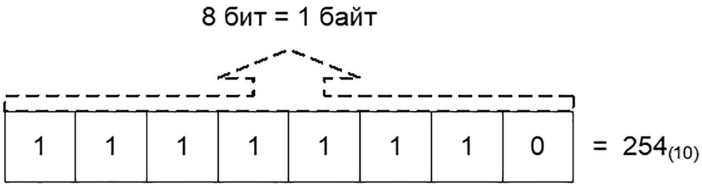


Рис. 1. Представление числа в десятичной системе счисления

Человеку удобнее работать с данными в десятичной СС, а для чтения информации применяются специальные таблицы преобразования – так называемые ASCII-таблицы,

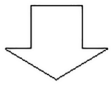
которые содержат в себе соответствие бинарного кода, представленного в шестнадцатеричной СС, буквенно-цифирному обозначению (рис. 2) [5].

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.A	.B	.C	.D	.E	.F
0.	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	SO	SI
1.	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2.		!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
3.	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4.	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5.	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6.	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7.	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	DEL

Рис. 2. ASCII-таблица

Возьмем в качестве атомарной единицы преобразования (далее – АЕП) данных величину, равную размеру одного ASCII-символа – 1 байт (рис. 3). Таким образом, всю информацию, хранящуюся на цифровом носителе, можно представить в виде последовательного массива символов и наглядно ее отобразить.

21	34	52	2B	47	69	4F	71
40	44	24	6D	3E	57	7A	59
37	3A	6A	54	7C	62	3D	23



!	4	R	+	G	i	O	q
@	D	$	m	>	W	z	Y
7	:	j	T	|	b	=	#

Рис. 3. Пример ASCII-символов

Блоком для преобразования будет служить трехмерный массив, размерностью 3×3×3, в ячейках которого будет находиться АЕП и дополнительные коды. Внешне описанный массив схож с механической головоломкой, изобретенной венгерским скульптором и преподавателем архитектуры Эрнё Рубиком, – кубиком Рубика (рис. 4) [6]. Таким образом, размер блока составляет 27 байт.

Внешнее сходство логической модели куба с механической головоломкой Эрнё Рубиком неспроста.

В качестве дополнительных кодов будут выступать тройки псевдослучайных чисел, размерностью равной АЕП – 1 байт (рис. 5). Это позволит всегда формировать различные зашифрованные данные при одинаковом ключе и исходных данных.

В результате входные данные разбиваются на блоки по 24 байта, к которым добавляются 3 байта случайных чисел. Затем каждый такой набор собирается в трехмерный массив. При этом расположение случайных чисел в массиве задается ключом шифрования из восьми возможных вариантов взаимно непересекающихся осей (рис. 6).

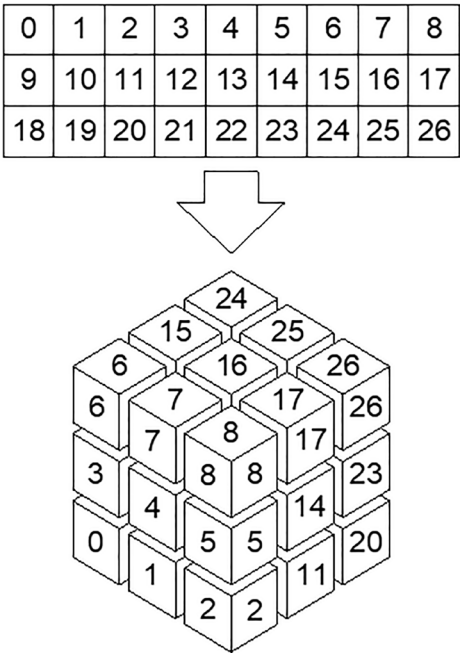


Рис. 4. Сборка логической модели куба

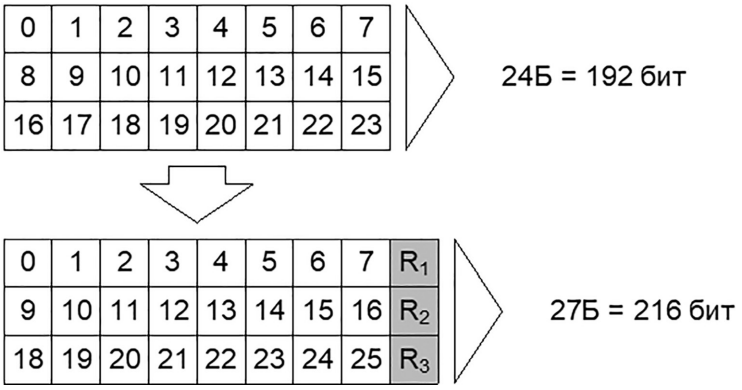


Рис. 5. Блок шифрования

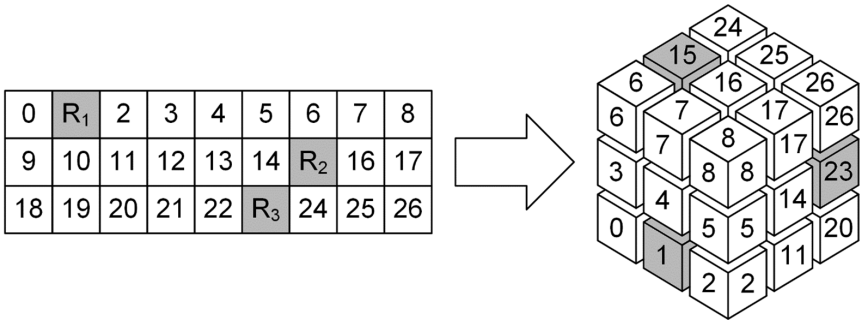


Рис. 6. Индексы случайных чисел

На рисунке 6 представлен вариант расположения случайных чисел. Остальные индексы выбираются подобным образом.

После сборки логической модели куба происходит циклическое вращение взаимно перпендикулярных граней с применением одного из двух разновидностей математического сложения по модулю равной мощности алфавита (в нашем случае $2^8 = 256$) всех кодов и наложением предварительно сформированных гамм [8] (рис. 7–8).

$A_1' = A_1$
$A_2' = A_1 + A_2$
$A_3' = A_1 + A_2 + A_3$

$A_1 = A_1'$
$A_2 = A_2' - A_1'$
$A_3 = A_3' - A_2'$

A_1	85	85	85 = 85
A_2	76	161	161 = 85 + 76
A_3	240	145	145 = 85 + 76 + 240 - 256

Рис. 7. Вариант сложения № 1 без гаммирования

$A_1' = A_1$
$A_2' = A_1 + A_2$
$A_3' = A_1 + A_2' + A_3$

$A_1 = A_1'$
$A_2 = A_2' - A_1'$
$A_3 = A_3' - A_2' - A_1'$

A_1	85	85	85 = 85
A_2	76	161	161 = 85 + 76
A_3	240	230	230 = 85 + 161 + 240 - 256

Рис. 8. Вариант сложения № 2 без гаммирования

Наложение гаммы производится на слой A_1 до применения математического преобразования всех кодов [10]. Таким образом, гамма будет накладываться на весь куб через слой A_1, поскольку остальные слои (A_2 и A_3) имеют от него математическую зависимость [11].

Порядок вращения ребер кубика с математическим преобразованием определяется ключом шифрования (рис. 9) таким образом, чтобы одна итерация составляла:

1. Определение слоя A_1 (ребро кубика).
2. Наложение гаммы на слой A_1.
3. Сложение всех кодов одним из вариантов (задается ключом) математического преобразования.
4. Вращение слоя A_1 вокруг своей оси (поворот задается ключом).
5. Выбор нового слоя A_1 перпендикулярно предыдущему.
6. Повторение пунктов 2–4.
7. Выбор следующего слоя A_1 взаимно перпендикулярно двум предыдущим.
8. Повторение пунктов 2–4.
9. При этом количество итераций и выбор взаимно перпендикулярных ребер определяется ключом шифрования.

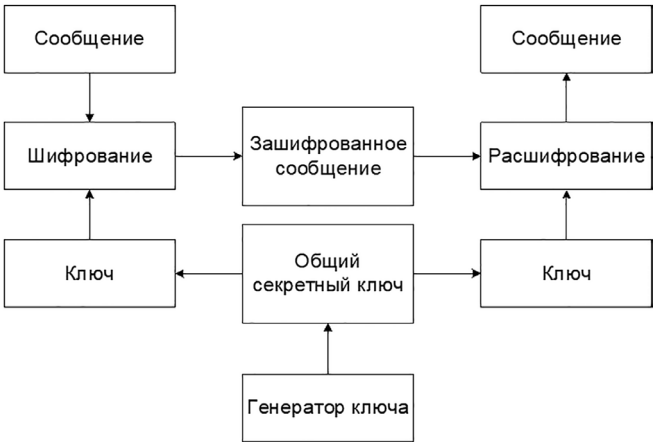


Рис. 9. Общая схема симметричного метода шифрования

Краткое описание программного комплекса

Программный комплекс включает в себя графический интуитивно понятный интерфейс на русском языке, написанный с помощью SDK Qt Designer, набор предустановленных гамм для начальной настройки шифрования и набор словарей нового алфавита. Написан на C++ с использованием кроссплатформенного фреймворка Qt.

Программа предназначена для повышения защищенности автоматизированных систем и сетей путем шифрования файлов данных оригинальным алгоритмом.

Обеспечивает выполнение следующих функций:

- создание, изменение и удаление файлов из автоматизированной системы (в режиме текстового редактора);
- выбор чтения исходных данных из файла либо из текстового поля программы;
- выбор чтения ключа шифрования (дешифрования) из файла либо из текстового поля программы (с ограничениями на минимальную длину);
- формирование управляющего вектора преобразования данных;
- подготовка исходных данных для преобразования;
- расчет и разделение исходных данных на блоки фиксированной ширины;
- выборка и преобразование блока исходных данных;
- конкатенация преобразованных блоков данных;
- вывод результата в файл или текстовое окно программы.

Главное окно программы изображено на рисунке 10 и состоит из основного поля, меню и служебных кнопок.

Меню содержит в себе 5 вкладок:

1. Файл
   a. Создать Ctrl+N
   b. Открыть… Ctrl+O
   c. Сохранить Ctrl+s
   d. Сохранить как… Ctrl+Alt+S
   e. Закрыть
   f. Выход Ctrl+Q

2. Действие
   a. Шифровать Ctrl+E
   b. Расшифровать Ctrl+D
3. Данные
   a. Ввести F4
   b. Выбрать файл… F5
   c. Этот файл
4. Ключ
   a. Ввести F8
   b. Считать из файла F9
5. Справка
   a. Содержание… F11
   b. О программе… F12

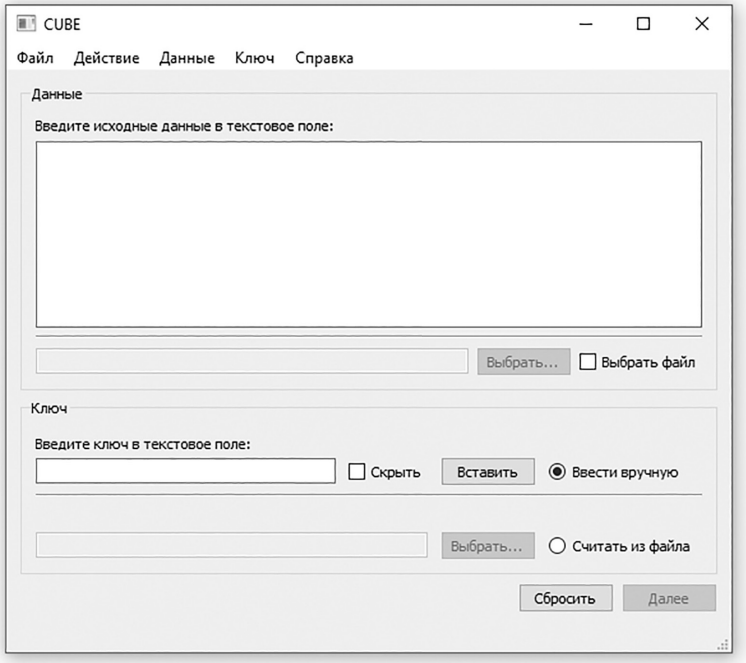


Рис. 10. Главное окно программы

Основное поле содержит форму для выбора ввода данных или чтения их из файла. Особенностью является блокировка соответствующего поля при нажатии на переключатель. При вводе пароля в текстовом формате присутствует возможность скрыть его отображение.

Служебными кнопками являются кнопка «Сбросить» – очищает все поля и приводит переключатели в исходное положение, и кнопка «Далее» – активируется только после правильного ввода всех необходимых данных.

В режим текстового редактора можно перейти при выборе пункта меню «Создать» или «Открыть» рисунке 11. Данный режим позволяет просматривать содержимое файлов в текстовом формате, изменять, сохранять и создавать документы. При нажатии на

пункт меню «Этот файл» программа помещает содержимое текстового поля в исходные данные и возвращает режим главного окна.

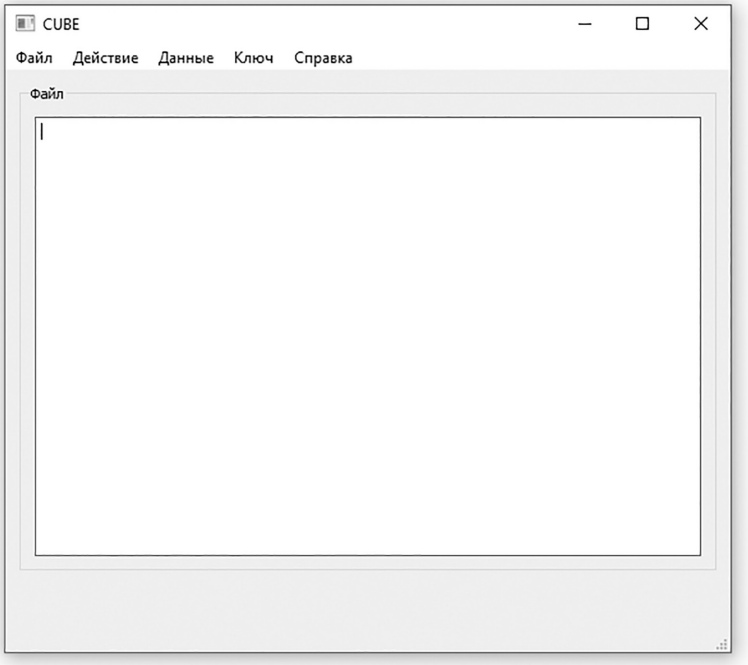


Рис. 11. Окно текстового редактора

При нажатии пунктов меню «Выбрать файл… » или «Считать из файла» либо соответствующих кнопок в основном поле программы появляется диалоговое окно выбора файла (рис. 12).

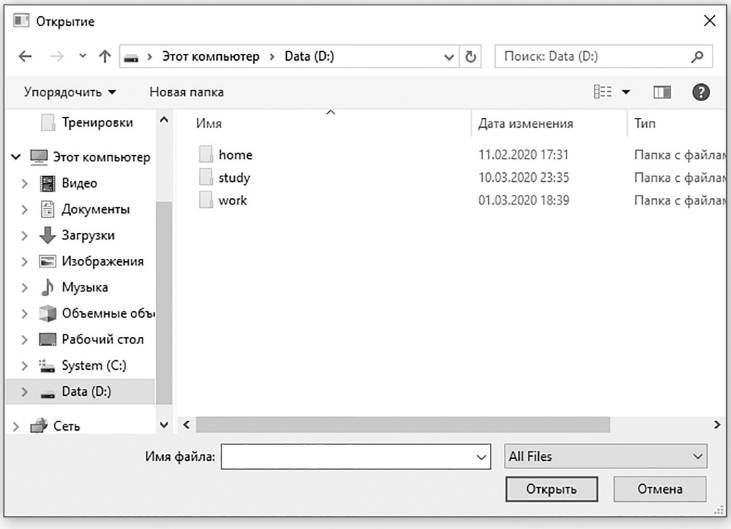


Рис. 12. Окно выбора файла

Заключение

Разработанный алгоритм симметричного шифрования обладает высоким быстродействием. Криптостойкость алгоритма зависит от размера ключа, минимальный размер которого составляет 256 бит. Методом грубой силы извлечь полезную информацию из зашифрованного сообщения невозможно без наличия гамм и алфавитов преобразования.

Развитием данной модели является децентрализованная информационная система защищенного обмена данных на основе предложенного алгоритма с добавлением функций генерации гамм на каждой стороне, динамического выбора алфавитов преобразования без передачи этих данных другим лицам. Реализовать подобную систему представляется возможным благодаря использованию трехэтапного протокола Кака. Основная идея этого метода заключается в отправке секретов через ненадежный канал, когда оба – Алиса и Боб – шифруют передаваемый секрет, который также называется криптографией с двойным замком. Алиса шифрует секрет своим ключом, отправляет Бобу, Боб его также шифрует и отправляет Алисе, после чего Алиса расшифровывает его своим ключом и опять отправляет Бобу, Боб расшифровывает своим и получает секрет.

Можно сделать вывод, что оригинальный алгоритм шифрования имеет большой потенциал применения его в защищенных системах передачи данных. Существует множество вариантов усовершенствования логической модели куба и математического преобразования над ним, что приведет к увеличению криптостойкости.

Литература

1. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М.: Госстандарт России, 1989.

2. *Нечай А.А.* Кибербезопасность и информационная безопасность: сущность, содержание и отличие понятий // XXIV Царскосельские чтения. 75-летие Победы в Великой Отечественной войне: материалы Международной научной конференции / под общ. ред. С.Г. Еремеева. СПб., 2020. С. 229–232.

3. *Нечай А.А.* Формирование безопасной информационной среды // Актуальные проблемы современности: наука и общество. 2019. № 4 (25). С. 43–44.

4. *Нечай А.А., Котиков П.Е.* Актуальные проблемы защиты информации в современных автоматических телефонных станциях // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2015. Вып. 2. С. 65–69.

5. *Нечай А.А., Котиков П.Е.* Методика комплексной защиты данных, передаваемых и хранимых на различных носителях информации // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2015. Вып. 1. С. 92–95.

6. *Сегеди А.* Великие венгры: Эрнё Рубик // Будапешт. Жемчужина Дуная / под ред. И.В. Осанова. М.: Вече, 2012. 320 с.

7. *Спесивцев А. В. и др.* Защита информации в персональных ЭВМ. М.: Радио и связь: МП «Веста», 1992. 192 с. (Библиотека системного программиста).

8. *Шаймарданов А.М., Нечай А.А., Лепехин С.В.* Математические модели систем автоматического управления с широтно-импульсной модуляцией // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2019. Вып. 2. С. 27–39.

9. *Эсаулов К.А., Яхваров Е.К., Нечай А.А., Березин А.С.* Методика интеграции системы управления киберрисками в предпринимательских структурах // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2020. Вып. 2. С. 80–86.

10. ISO/IEC 8859-5:1999 // ISO. URL: https://www.iso.org/standard/28249.html (дата обращения: 10.04.2020).

11. *Popov V., Kurepkin I., Leontiev S.* Additional Cryptographic Algorithms for Use with GOST 28147–89, GOST R 34.10–94, GOST R 34.10–2001, and GOST R 34.11–94 Algorithms // RFC 4357. IETF, January 2006.

Literatura

1. GOST 28147–89. Sistemy obrabotki informatsii. Zashchita kriptograficheskaya. Algoritm kriptograficheskogo preobrazovaniya. M.: Gosstandart Rossii, 1989.

2. *Nechaj A.A.* Kiberbezopasnost' i informatsionnaya bezopasnost': sushchnost', soderzhanie i otlichie ponyatij // XXIV Tsarskosel'skie chteniya. 75-letie Pobedy v Velikoj Otechestvennoj vojne: materialy Mezhdunarodnoj nauchnoj konferentsii / pod obshch. red. S.G. Eremeeva. SPb., 2020. S. 229–232.

3. *Nechaj A.A.* Formirovanie bezopasnoj informatsionnoj sredy // Aktual'nye problemy sovremennosti: nauka i obshchestvo. 2019. № 4 (25). S. 43–44.

4. *Nechaj A.A., Kotikov P.E.* Aktual'nye problemy zashchity informatsii v sovremennykh avtomaticheskikh telefonnykh stantsiyakh // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2015. Vyp. 2. S. 65–69.

5. *Nechaj A.A., Kotikov P.E.* Metodika kompleksnoj zashchity dannykh, peredavaemykh i khranimykh na razlichnykh nositelyakh informatsii // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2015. Vyp. 1. S. 92–95.

6. *Segedi A.* Velikie vengry: Ernyo Rubik // Budapesht. Zhemchuzhina Dunaya / pod red. I.V. Osanova. M.: Veche, 2012. 320 s.

7. *Spesivtsev A. V. i dr.* Zashchita informatsii v personal'nykh EVM. M.: Radio i svyaz': MP "Vesta", 1992. 192 s. (Biblioteka sistemnogo programmista).

8. *Shajmardanov A.M., Nechaj A.A., Lepekhin S.V.* Matematicheskie modeli sistem avtomaticheskogo upravleniya s shirotno-impul'snoj modulyatsiej // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2019. Vyp. 2. S. 27–39.

9. *Esaulov K.A., Yakhvarov E.K., Nechaj A.A., Berezin A.S.* Metodika integratsii sistemy upravleniya kiberriskami v predprinimatel'skikh strukturakh // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2020. Vyp. 2. S. 80–86.

10. ISO/IEC 8859-5:1999 // ISO. URL: https://www.iso.org/standard/28249.html (data obrashcheniya: 10.04.2020).

11. *Popov V., Kurepkin I., Leontiev S.* Additional Cryptographic Algorithms for Use with GOST 28147–89, GOST R 34.10–94, GOST R 34.10–2001, and GOST R 34.11–94 Algorithms // RFC 4357. IETF, January 2006.

Выпуск 3/2020

DOI: 10.25586/RNU.V9187.20.03.P.100 УДК 004

Ю.Л. Плеханов, И.Ш. Шафигуллин

ПРЕДЛОЖЕНИЯ ПО ФОРМИРОВАНИЮ БАЗЫ ЗНАНИЙ ЭКСПЕРТНОЙ СИСТЕМЫ ПУНКТОВ УПРАВЛЕНИЯ ДЛЯ РЕШЕНИЯ ЗАДАЧ СИТУАЦИОННОГО УПРАВЛЕНИЯ

Описываются особенности применения экспертных систем как комплексов программных средств, реализующих методы и технологии искусственного интеллекта, основанные на знаниях. Выдвинуты предложения по формирования базы знаний пункта управления для решения задач ситуационного управления.

Ключевые слова: кризисная ситуация, ситуационное управление, пункт управления, база знаний, экспертная система.

Yu.L. Plekhanov, I.Sh. Shafigullin

PROPOSAL FOR THE FORMATION OF THE KNOWLEDGE BASE OF THE EXPERT SYSTEM OF THE CONTROL POST TO SOLVE THE PROBLEMS OF SITUATIONAL MANAGEMENT

The features of the use of expert systems as complexes of software tools that implement the methods and technologies of artificial intelligence based on knowledge are described. Proposals are put forward for the formation of a knowledge base of the control point for solving problems of situational control.

Keywords: crisis situation, situational management, control post, knowledge base, expert system.

Известно, что оперативный состав пунктов управления (ПУ) войсковых формирований различного уровня в ходе сложной динамично изменяющейся обстановки при решении задач ситуационного управления сталкивается с переработкой все более увеличивающегося объема поступающей информации [2], проведением объемных вычислительных действий в условиях острого дефицита времени. При этом задачи ситуационного управления зачастую отличаются наличием большого числа неструктурированных (слабоструктурированных) данных [10]. В этой связи одним из наиболее перспективных и ресурсосберегающих направлений реализации имеющихся резервов повышения качества управления и оперативности принятия управленческих решений на ПУ при решении таких сложных задач является применение методов и технологий искусственного интеллекта [13]. Отдельным его самостоятельным направлением являются экспертные системы (ЭС) или инженерия знаний, т.е. системы, позволяющие на базе современных компьютеров накапливать, обновлять и корректировать знания из различных предметных областей. Экспертные системы могут быть отнесены к системам, которые не только исполняют заданные процедуры, но на основе метапроцедур поиска генерируют и используют процедуры решения новых конкретных задач, например, анализ ситуаций, принятие решений в условиях неопределенности (неполноты информации), краткосрочное прогнозирование [5]. Одним из основных элементов ЭС является база знаний, предназначенная