INFORMATION SYSTEMS ИНФОРМАЦИОННЫЕ СИСТЕМЫ

УДК 519.718

С.А. Диченко, О.А. Финько

СНИЖЕНИЕ ВВОДИМОЙ ИЗБЫТОЧНОСТИ ПРИ ОБЕСПЕЧЕНИИ УСТОЙЧИВОСТИ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ В УСЛОВИЯХ КОМПЕНСАЦИИ ПОСЛЕДСТВИЙ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ ЗЛОУМЫШЛЕННИКА

***Диченко Сергей Александрович**, кандидат технических наук, окончил Краснодарское высшее военное училище им. ген. армии С.М. Штеменко. Докторант Краснодарского высшего военного училища им. ген. армии С.М. Штеменко. Имеет статьи, изобретения в области безопасности информации, систем криптокодовой защиты информации, модулярной арифметики многомерных числовых систем. [e-mail: dichenko.sa@yandex.ru].*

***Финько Олег Анатольевич**, доктор технических наук, профессор, окончил Ставропольское высшее военное инженерное училище связи. Профессор Краснодарского высшего военного училища им. ген. армии С.М. Штеменко. Имеет статьи, изобретения в области параллельных вычислений в системе остаточных классов, числовой реализации систем функций алгебры логики, функционального диагностирования цифровых устройств избыточными кодами, контроля целостности информации в системах электронного документооборота и других информационных системах, аспектов инженерной реализации криптографических примитивов, систем счисления. [e-mail: ofinko@yandex.ru].*

Аннотация

Рассматриваются информационно-аналитические системы (ИАС), в основе функционирования которых лежит обработка больших многомерных массивов информации в условиях деструктивных воздействий злоумышленника. Для таких условий функционирования одной из актуальнейших задач является организация безопасного хранения данных, обеспечивающая тождественность данных у оператора, отправившего их на хранение, и у лица, принимающего решение, при запросе на их использование. Предложена подсистема контроля целостности данных, основанная на применении криптографических хэш-функций. Применение функции хэширования в разработанной подсистеме основано на правилах построения треугольника Паскаля. Показано, что особенностью разработанной подсистемы является снижение вводимой избыточности контрольной информации при заданном уровне защищенности данных, обрабатываемых в ИАС, а также обеспечение ее новыми свойствами: возможностью осуществления контроля целостности не только данных, подлежащих защите, но и самих эталонных хэш-кодов. Представлена сравнительная оценка разработанной подсистемы с известными способами контроля целостности данных.

Ключевые слова: информационно-аналитическая система, защита информации, контроль целостности данных, хэш-функция, хэш-код, треугольник Паскаля.

doi: 10.35752/1991-2927-2020-4-62-38-48

REDUCED INPUT REDUNDANCY WHILE PROVIDING THE STABILITY OF INFORMATION-ANALYTICAL SYSTEMS IN COMPENSATING THE EFFECTS CAUSED BY ATTACKER'S DESTRUCTIVE ACTIONS

Sergei Aleksandrovich Dichenko, Candidate of Sciences in Engineering; graduated from Shtemenko Krasnodar Higher Military School; Postdoctoral Student of Shtemenko Krasnodar Highest Military School; an author of articles, inventions in the field of information security, crypto-code information security systems, modular arithmetic of multidimensional numerical systems. e-mail: dichenko.sa@yandex.ru.

Oleg Anatolevich Finko, Doctor of Sciences in Engineering, Professor; graduated from the Stavropol Higher Military Engineering School of Communications; Professor of Shtemenko Krasnodar Higher Military School; an author of articles, inventions in the field of parallel computing in the system of residual classes, numerical implementation of systems of functions of logic algebra, functional diagnostics of digital devices with redundant codes, control of information integrity in systems. e-mail: ofinko@yandex.ru.

Abstract

The article describes the information and analytical systems (IAS), the main function of which is processing of large multidimensional arrays of information under conditions of destructive effects caused by attacker. Such conditions require the management of secure data storage. It ensures the data sent for storage by operator is identical to the one used by a decision-maker upon request. The authors propose the subsystem of data integrity control that uses cryptographic hash functions. The applied hash functions are based on the rules for constructing Pascal's triangle. The paper shows that a distinguishing feature of the subsystem is reducing the input redundancy of control information at a given security level of data processed in the IAS, as well as ensuring new properties, such as the ability to control the integrity of not only the data to be secured, but also the reference hash codes. The article also gives a comparative assessment of the developed subsystem with known methods of data integrity control.

Keywords: information and analytical system, information security, data integrity control, hash function, hash code, the Pascal's triangle.

ВВЕДЕНИЕ

В современных условиях эволюционного роста объема и ценности информации, обрабатываемой в информационных системах различного назначения, функционирующих в условиях деструктивных воздействий злоумышленника, вопросы обеспечения их устойчивости оставались до последнего времени, по нашему мнению, без должного глубокого научного изучения. Среди немногих известны работы [1–4], в которых задача построения устойчивых информационных систем решалась исключительно через обеспечение их живучести, надежности и помехоустойчивости, однако при этом вопросы безопасности информации, обрабатываемой в информационных системах или хранящейся в системах хранения данных, остаются без должного внимания.

В настоящее время для обеспечения устойчивости информационно-аналитических систем (ИАС) в условиях деструктивных воздействий злоумышленника перед их пользователями стоят задачи по защите обрабатываемых в них данных. Одной из мер обеспечения сохранности данных, обрабатываемых в информационных системах, является защита их целостности [5]. Задача защиты целостности данных является сложной, ввиду своей комплексности, так как включает в себя не только восстановление данных, целостность которых была

нарушена, но и предшествующий этой процедуре контроль.

Одним из известных и широко используемых способов контроля целостности данных является применение криптографических методов, в частности, функции хэширования [6–8]. Однако, несмотря на повсеместное применение хэш-функций, информации о них гораздо меньше, чем, к примеру, о блочных шифрах [9]. В сравнении с блочными шифрами хэш-функции крайне мало исследованы, а практические предложения по их применению весьма немногочисленны [10–15].

1 АНАЛИЗ СУЩЕСТВУЮЩИХ СПОСОБОВ ПРИМЕНЕНИЯ ХЭШ-ФУНКЦИИ

Известны различные способы применения хэш-функций для контроля целостности данных, подлежащих защите. На рисунке 1 представлена классификация способов применения хэш-функции к данным, выполненная в зависимости от состава и порядка вычисления хэш-кодов.

1) Способ применения хэш-функции h для k блоков данных, представленных двоичными векторами $\mathbf{M}_i$ ($i = 1, 2, \dots, k$), с вычислением одного общего хэш-кода $\mathbf{H}$: $h(\mathbf{M}_1, \mathbf{M}_2, \dots, \mathbf{M}_k) = \mathbf{H}$, поясняется на рисунке 2.

Рис. 1. Классификация способов применения хэш-функции к данным

Рис. 2. Способ применения хэш-функции для k блоков данных с вычислением одного общего хэш-кода

Достоинство: низкая избыточность.

Недостатки:

- отсутствие возможности локализации блока данных, представленного двоичным вектором $\mathbf{M}_i$, при контроле целостности данных;
- малая вероятность обнаружения ошибки (определения факта нарушения целостности данных) при пропуске ошибки (ложном сигнале об ошибке) средствами контроля.

2) Способы применения хэш-функции для k блоков данных с вычислением n хэш-кодов (при $k \geq n$) подразделяются на:

2.1) способы применения хэш-функции (при $k = n$), которые в свою очередь можно подразделить на следующие:

а) способ применения хэш-функции, при котором от каждого из блоков данных, представленных двоичными векторами $\mathbf{M}_i$, вычисляется свой хэш-код $\mathbf{H}_i$;

б) способ применения полносвязной сети хэширования, где каждый хэш-код $\mathbf{H}_i$ вычисляется от всей совокупности блоков данных, представленных двоичными векторами $\mathbf{M}_i$;

2.2) способы применения хэш-функции (при $k > n$).

Способ применения хэш-функции h , при котором от каждого из блоков данных, представленных двоичными векторами $\mathbf{M}_i$, вычисляется хэш-код $\mathbf{H}_i$: $h(\mathbf{M}_i) = \mathbf{H}_i$, поясняется на рисунке 3.

Рис. 3. Способ применения хэш-функции, при которой от каждого из блоков данных вычисляется хэш-код

В этом случае, количество вычисленных хэш-кодов $\mathbf{H}_i$ будет равняться количеству двоичных векторов $\mathbf{M}_i$.

Достоинства:

- простота реализации;
- возможность локализации блока данных, представленного двоичным вектором $\mathbf{M}_i$, при контроле целостности данных.

Недостатки:

- высокая избыточность при контроле целостности блоков данных, представленных двоичными векторами небольшой размерности;
- малая вероятность обнаружения ошибки (определения факта нарушения целостности данных) при пропуске ошибки (ложном сигнале об ошибке) средствами контроля.

Способ применения полносвязной сети хэширования, где каждый хэш-код $\mathbf{H}_i$ вычисляется от всей сово-

купности блоков данных, представленных двоичными векторами $\mathbf{M}_i$: $h(\mathbf{M}_1 \parallel \mathbf{M}_2 \parallel \dots \parallel \mathbf{M}_k) = \mathbf{H}_i$, поясняется на рисунке 4.

Рис. 4. Способ применения полносвязной сети хэширования

В данном способе большое значение имеет последовательность блоков данных, представленных двоичными векторами $\mathbf{M}_i$, участвующих в конкатенации (объединении). Здесь первым объединяется блок данных, представленный двоичными векторами $\mathbf{M}_i$, номер которого соответствует номеру вычисляемого хэш-кода $\mathbf{H}_i$ (за счет этого их значения будут отличаться между собой).

Например,

– при $i = 1$:

$$\mathbf{H}_1 = h(\mathbf{M}_1 \parallel \mathbf{M}_{i+1} \parallel \dots \parallel \mathbf{M}_k);$$

– при $i = 2$:

$$\mathbf{H}_2 = h(\mathbf{M}_2 \parallel \mathbf{M}_{i-1} \parallel \mathbf{M}_{i+1} \parallel \dots \parallel \mathbf{M}_k);$$

– при $i = k$:

$$\mathbf{H}_i = h(\mathbf{M}_i \parallel \mathbf{M}_{i-k+1} \parallel \mathbf{M}_{i-k+2} \parallel \dots \parallel \mathbf{M}_{k-1}), \text{ где } \parallel \text{ – операция конкатенации.}$$

Достоинство: повышение вероятности обнаружения ошибки (определения факта нарушения целостности данных) при пропуске ошибки (ложном сигнале об ошибке) средствами контроля.

Недостатки:

– высокая избыточность при контроле целостности блоков данных, представленных двоичными векторами небольшой размерности;

– в общем виде данная схема не позволяет выполнить локализацию блока данных в случае нарушения его целостности.

Однако частные случаи способа применения функции хэширования (рис. 4) позволяют локализовать блок данных с нарушением целостности с одновременным снижением вводимой избыточности, в отличие от способов, представленных на рисунках 2 и 3.

В свою очередь, при контроле целостности данных наибольший интерес представляют способы применения хэш-функции (при $k > n$). В [16] представлено

решение, позволяющее обеспечить локализацию искаженных или утраченных блоков данных, подлежащих защите, с одновременным снижением избыточности контрольной информации при осуществлении контроля целостности данных в автоматизированных системах, где с помощью математического аппарата теории систем векторов выполнено обоснование и разработка алгоритма построения линейных систем хэш-кодов, правила (принципы) построения которых аналогичны правилам построения линейных избыточных кодов, в частности кодов Хемминга.

Известны другие способы применения хэш-функции, позволяющие локализовать блоки данных, с нарушенной целостностью с одновременным снижением вводимой избыточности [17–19]. Эти способы, основанные на схемах построения помехоустойчивых кодов, учитывают структуру многомерного представления информации в современных системах хранения данных ИАС.

Одним из главных недостатков представленных способов является отсутствие возможности определения факта нарушения целостности данных в условиях искажения самой контрольной информации, что может привести к пропуску ошибки или ложному сигналу об ошибке.

Разработанная подсистема контроля целостности данных позволяет устранить недостатки существующих способов: уменьшить избыточность контрольной информации, а также обеспечить контроль целостности самих эталонных хэш-кодов (контрольной информации) за счет оригинальности схемы применения хэш-функций к блокам данных, подлежащих защите, основанной на правилах построения треугольника Паскаля [20].

2 РАЗРАБОТКА ПОДСИСТЕМЫ КОНТРОЛЯ ЦЕЛОСТНОСТИ ДАННЫХ, ОСНОВАННОЙ НА ПРАВИЛАХ ПОСТРОЕНИЯ ТРЕУГОЛЬНИКА ПАСКАЛЯ

Схема применения хэш-функции к блокам данных на основе криптографического треугольника Паскаля представлена на рисунке 5 и содержит таблицу, имеющую треугольную форму.

В этом треугольнике по бокам размещены блоки $\mathbf{M}_{ij}$ ($i = 1, 2, \dots, n$; $j = 1, 2$), подлежащие защите, внутри треугольника – промежуточные результаты преобразований – хэш-коды, вычисляемые от защищаемых блоков данных и (или) хэш-кодов, вычисляемых на предыдущем уровне, к примеру:

$$\mathbf{H}_{11} = h(\mathbf{M}_{11}, \mathbf{M}_{12}), \dots, \mathbf{H}_{t1} = h(\mathbf{M}_{t1}, \mathbf{H}_{t-1,1}), \dots,$$

внизу – значения хэш-кодов $\mathbf{H}_{ij}$ ($i, j = 1, 2, \dots, n$), которые вычисляются от блоков $\mathbf{M}_{n1}$ и $\mathbf{M}_{n2}$, подлежащих защите, и результатов промежуточных преобразований нижнего уровня:

$$\mathbf{H}_{n-1,1}, \mathbf{H}_{n-1,2}, \dots, \mathbf{H}_{n-1,n-1};$$

где $\mathbf{H}_{n+1,1}, \mathbf{H}_{n+1,2}, \mathbf{H}_{n+1,3}$ – эталонные хэш-коды второго порядка, вычисляемые соответственно по формулам:

Рис. 5. Общая схема применения хэш-функции, основанная на правилах построения треугольника Паскаля

$$H_{n+1,1} = h(M_{12}, M_{22}, M_{32}, \dots, M_{t2}, M_{t+1,2}, \dots, M_{n2}, H_{n+1,3}),$$

$$H_{n+1,2} = h(H_{n+1,1}, M_{11}, M_{21}, M_{31}, \dots, M_{t1}, M_{t+1,1}, \dots, M_{n1}),$$

$$H_{n+1,3} = h(H_{n+1,2}, H_{n1}, H_{n2}, \dots, H_{nn}).$$

Контроль целостности блоков M_{ij} осуществляется путем сравнения значений, вычисленных при запросе на использование защищаемых данных хэш-кодов, со значениями эталонных хэш-кодов $H_{n1}, H_{n2}, \dots, H_{nn}$, вычисленных ранее.

Для контроля целостности эталонных хэш-кодов вычисляется эталонный хэш-код второго порядка (рис. 6).

Рис. 6. Схема контроля целостности эталонных хэш-кодов

Пример 1. Для блока данных (при $n = 5$) схема применения хэш-функции, основанная на правилах построения треугольника Паскаля, примет вид (рис. 7):

Рис. 7. Схема применения хэш-функции, основанная на правилах построения треугольника Паскаля (при $n = 5$)

Контроль целостности (локализация) блока данных осуществляется при построении сети хэширования.

Сеть хэширования для схемы, представленной на рисунке 7, примет вид (рис. 8).

Пример 2. Сеть хэширования для схемы применения хэш-функции (при $n = 5$), примет вид (рис. 9).

На основе сети хэширования (рис. 9) составляется таблица.

На основе полученного синдрома принимается решение об искаженном или утраченном блоке данных.

3 Модифицированная подсистема контроля целостности данных на основе правил построения пирамиды Паскаля

Схема применения хэш-функции к блокам данных на основе криптографической пирамиды Паскаля представлена на рисунке 10.

Кроме сокращения вводимой избыточности контрольной информации, представленной конструкции присущи отличительные свойства, связанные с увели-

Рис. 8. Общий вид сети хэширования для схемы применения хэш-функции

Рис. 9. Сеть хэширования для схемы применения хэш-функции к блоку данных (при $n = 5$)

Таблица

Таблица синдромов для локализации однократной ошибки

Синдром								Локализация ошибки
H_{63}	H_{62}	H_{61}	H_{55}	H_{54}	H_{53}	H_{52}	H_{51}	Результат
			0	0	0	0	0	Нет ошибки
0	0	0	1	0	0	0	0	$M_{11}, \dots, M_{51}, [\widetilde{M}_{52}]$
0	0	0	0	0	0	0	1	$M_{11}, \dots, M_{42}, [\widetilde{M}_{51}], M_{52}$
0	0	0	1	1	0	0	0	$M_{11}, \dots, M_{41}, [\widetilde{M}_{42}], M_{51}, M_{52}$
0	0	0	0	0	0	1	1	$M_{11}, \dots, M_{32}, [\widetilde{M}_{41}], M_{42}, M_{51}, M_{52}$
0	0	0	1	1	1	0	0	$M_{11}, \dots, M_{31}, [\widetilde{M}_{32}], M_{41}, \dots, M_{52}$
0	0	0	0	0	1	1	1	$M_{11}, \dots, M_{22}, [\widetilde{M}_{31}], M_{32}, \dots, M_{52}$
0	0	0	1	1	1	1	0	$M_{11}, M_{12}, M_{21}, [\widetilde{M}_{22}], M_{31}, \dots, M_{52}$
0	0	0	0	1	1	1	1	$M_{11}, M_{12}, [\widetilde{M}_{21}], M_{22}, \dots, M_{52}$
0	0	1	1	1	1	1	1	$M_{11}, [\widetilde{M}_{12}], M_{21}, \dots, M_{52}$
0	1	0	1	1	1	1	1	$M_{11}, M_{12}, [\widetilde{M}_{21}], M_{22}, \dots, M_{52}$
-	1	-	0	0	0	0	0	$[\widetilde{H}_{61}]$
-	-	1	0	0	0	0	0	$[\widetilde{H}_{63}]$
1	-	-	0	0	0	0	0	$[\widetilde{H}_{62}]$ или $[\widetilde{H}_{5j}]$

чением кратности гарантированно обнаруживаемых и локализуемых блоков данных в случае нарушения их целостности.

4 ОЦЕНИВАНИЕ РАЗРАБОТАННОЙ ПОДСИСТЕМЫ КОНТРОЛЯ ЦЕЛОСТНОСТИ ДАННЫХ, ОСНОВАННОЙ НА ПРАВИЛАХ ПОСТРОЕНИЯ ТРЕУГОЛЬНИКА ПАСКАЛЯ

При проектировании и разработке новых ИАС возникает задача нахождения оптимального решения для контроля целостности хранящейся в них информации, то есть обеспечения требуемой устойчивости ИАС через свойство безопасности информации. Для этого в качестве показателя качества определим объем вводимой избыточности – $V_{изб}$.

Критерий качества: $V_{изб} \rightarrow \min$.

Оценивание предложенной подсистемы контроля выполняется в сравнении со способами применения хэш-функции, способными локализовать искаженный или утраченный блок данных, при этом контрольная информация (избыточность), введенная для осуществле-

ния контроля целостности защищаемых данных, равна k (объем избыточности $V_{изб} = 100\%$).

В разработанной подсистеме для контроля целостности k блоков данных требуется вычислить $\frac{k}{2}$ хэш-кодов. К тому же, разработанная подсистема контроля позволяет при увеличении контрольной информации, в частности, на три эталонных хэш-кода $H_{n+1,1}, H_{n+1,2}, H_{n+1,3}$, осуществить контроль целостности самих хэш-кодов, тогда объем вводимой избыточности будет вычисляться в соответствии со следующим выражением:

$$V_{изб} = \frac{\frac{k}{2} + 3}{k}. \quad (1)$$

Пример 3. При $k = 10$ объем вводимой избыточности в соответствии с (1) будет равен: $V_{изб} = 80\%$; при $k = 12$: $V_{изб} = 75\%$; при $k = 100$: $V_{изб} = 53\%$.

Рис. 10. Общий вид криптографической пирамиды Паскаля

При увеличении количества блоков данных, подлежащих защите, избыточность, связанная с вычислением хэш-кодов, уменьшается.

ЗАКЛЮЧЕНИЕ

Таким образом, разработана подсистема контроля целостности данных на основе правил построения треугольника Паскаля. Результаты оценки показали, что разработанная подсистема контроля позволяет сократить избыточность, связанную с вычислением контрольной информации, при заданном уровне защищенности данных.

Предложенный подход позволяет осуществить контроль целостности не только данных, подлежащих защите, но и самих эталонных хэш-кодов (контрольной информации).

СПИСОК ЛИТЕРАТУРЫ

1. Модели и методы исследования информационных систем / А.Д. Хомоненко, А.Г. Басыров, В.П. Бубнов, А.В. Забродин, С.А. Краснов, В.А. Лохвицкий, А.В. Тырва. СПб. : Лань, 2019. 204 с.
2. Басыров А.Г., Захаров И.В. Оценивание живучести бортовых вычислительных систем космических аппара-

тов // Тр. Военно-космической академии им. А.Ф. Можайского. 2016. Вып. 651. С. 139–148.

3. Бучинский Д.И., Вознюк В.В., Фомин А.В. Исследование помехоустойчивости приемника сигналов с многопозиционной фазовой манипуляцией к воздействию помех с различной структурой // Тр. Военно-космической академии им. А.Ф. Можайского. 2019. Вып. 671. С. 120–127.

4. Флешман Б.С. Основы системологии. М. : Радио и связь, 1982. 368 с.

5. Omondi A., Premkumar B. *Residue Number System: Theory and Implementation*. London : Imperial College Press, 2007. 296 p.

6. Schneier B. *Applied Cryptography: Protocols, Algorithms and Source Code*. Second Edition. C. John Wiley & Sons, Inc. 2016. 653 p.

7. Menezes A.J., Oorschot P., Vanstone S. *Handbook of Applied Cryptography*. CRC Press, Inc. 2015. 770 p.

8. Knuth D.E. *The Art of Computer Programming: Volume 3: Sorting and Searching*. 2nd edn. 2018. 803 p.

9. Диченко С.А., Финько О.А. Алгоритм генерации блочной ПСП, основанный на применении логико-числовых форм // Известия ЮФУ. Технические науки. 2012. № 12 (137). С. 158–167.

10. Biham E., Dunkelman O. A framework for iterative hash functions: HAIFA // *Cryptology ePrint Archive*. Report 2007/278. 2007. pp. 1–20.

11. Wang X., Yu H. How to break MD5 and Other Hash Function // EUROCRYPT. LNCS 3494. Springer-Verlag, 2005. pp. 19–35.

12. Bellare M. New Proofs for NMAC and HMAC: Security without Collision-Resistance // *CRYPTO*. ePrint Archive. Report 2006/043. 2006. pp.1–16.

13. Финько О.А, Диченко С.А. Гибридный крипто-кодовый метод контроля и восстановления целостности данных для защищенных информационно-аналитических систем // Вопросы кибербезопасности. 2019. № 6 (34). С. 17–36.

14. Tchernykh A., Babenko M., Chervikov N. et al. AC-RRNS: Anti-Collusion Secured Data Sharing Scheme for Cloud Storage // *International Journal of Approximate Reasoning*. Special Issue on Uncertainty in Cloud Computing: Concepts, Challenges and Current Solutions. Vol. 102. pp. 60–73.

15. Tilborg H. *Fundamentals of cryptology: a professional reference and interactive tutorial*. Kluwer Academic Publishers. London, 2014. 414 p.

16. Диченко С.А. Контроль и обеспечение целостности информации в системах хранения данных // *Наукоемкие технологии в космических исследованиях Земли*. 2019. Т. 11, № 1. С. 49–57.

17. Пат. РФ 2485575. Самопроверяемый специализированный вычислитель систем булевых функций / Диченко С.А., Вишневецкий А.К., Финько О.А. Заявл. 18.05.2012. Оpubл. 20.06.2013. Бюл. № 17. 15 с.

18. Разработка алгоритма контроля и обеспечения целостности данных при их хранении в центрах обра-

ботки данных / С.А. Диченко, А.А. Жарких, А.А. Акилов, С.А. Кись // Информационный бюллетень Омского научно-образовательного центра ОмГТУ и ИМ СО РАН в области математики и информатики. Матер. VIII Междунар. молодеж. науч.-практ. конф. с элементами научной школы / отв. ред. А.В. Зыкина. Омск, 2018. С. 110–113.

19. Finko O.A., Dichenko S.A. Two-dimensional control and assurance of data integrity in information systems based on residue number system codes and cryptographic hash functions // *Proceedings of the 2018 Multidisciplinary Symposium on Computer Science and ICT*, Stavropol, Russia, October 15, 2018, 2254, CEUR Workshop Proceedings. 2018. pp. 139–146.

20. Гарднер М. Неисчерпаемое очарование треугольника Паскаля // *Математические новеллы*. М. : Мир, 1974. 456 с.

REFERENCES

1. Khomonenko A.D., Basyrov A.G., Bubnov V.P., Zabrodin A.V., Krasnov S.A., Lohvitskii V.A., Tyrva A.V. *Modeli i metody issledovaniia informatsionnykh sistem* [Models and Methods of Information System Research]. St. Petersburg, Lan Publ., 2019. 204 p.

2. Basyrov A.G., Zakharov I.V. Otsenivanie zhivuchesti bortovykh vychislitelnykh sistem kosmicheskikh apparatov [Estimation of Space-Borne Computer System Survivability]. *Tr. Voенno-kosmicheskoi akademii im. A.F. Mozhaiskogo* [Proc. of the Mozhaisky Military Space Academy]. 2016, iss. 651, pp. 139–148.

3. Buchinskii D.I., Vozniuk V.V., Fomin A.V. Issledovanie pomekhoustoichivosti priemnika signalov s mnogopozitsionnoi fazovoi manipuliatsiei k vozdeistviu pomekh s razlichnoi strukturoi [Research of Noise Stability of the Receiver with Multiposition Phase-Shift-Keying Modulation under the Influence of Interference with Different Structure]. *Tr. Voенno-kosmicheskoi akademii im. A.F. Mozhaiskogo* [Proc. of the Mozhaisky Military Space Academy]. 2019, iss. 671, pp. 120–127.

4. Fleishman B.S. *Osnovy sistemologii* [Fundamentals of Systemology]. Moscow, Radio i Sviaz Publ., 1982. 368 p.

5. Omondi A., Premkumar B. *Residue Number System: Theory and Implementation*. London, Imperial College Press, 2007. 296 p.

6. Schneier B. *Applied Cryptography: Protocols, Algorithms and Source Code*. Second Edition. C. John Wiley & Sons, Inc., 2016. 653 p.

7. Menezes A.J., Oorschot P., Vanstone S. *Handbook of Applied Cryptography*. CRC Press, 2015. 770 p.

8. Knuth D.E. *The Art of Computer Programming: Volume 3: Sorting and Searching*. 2nd edn. 2018. 803 p.

9. Dichenko S.A., Finko O.A. Algoritm generatsii blochnoi PSP, osnovannyi na primenenii logiko-chislovykh form [Algorithm for Generating Pseudorandom Sequence of Block Based on the Use Logical-Numeric Form]. *Izvestiia YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2012, no. 12 (137), pp. 158–167.

10. Biham E., Dunkelman O. A Framework for Iterative Hash Functions – HAIFA. *Cryptology ePrint Archive*, Report 2007/278, 2007, pp. 1–20.
11. Wang X., Yu H. How to Break MD5 and Other Hash Function. *Proc. of Annual International Conference on the Theory and Applications of Cryptographic Techniques. EUROCRYPT. LNCS 3494*. Springer-Verlag, 2005, pp. 19–35.
12. Bellare M. New Proofs for NMAC and HMAC: Security without Collision-Resistance. *CRYPTO. ePrint Archive*, Report 2006/043, 2006, pp. 1–16.
13. Finko O.A., Dichenko S.A. Gibridnyi krypto-kodovyi metod kontrolya i vosstanovleniya tselostnosti dannykh dlia zashchishchennykh informatsionno-analiticheskikh system [Hybrid Crypto-Code Method for Monitoring and Recovery of Data Integrity for Protected Information and Analytical Systems]. *Voprosy kiberbezopasnosti* [Cyber Security Issues Magazine], 2019, no. 6 (34), pp. 17–36.
14. Tchernykh A., Babenko M., Chervikov N. et al. AC-RRNS: Anti-Collusion Secured Data Sharing Scheme for Cloud Storage. *International Journal of Approximate Reasoning. Special Issue on Uncertainty in Cloud Computing: Concepts, Challenges and Current Solutions*, vol. 102, pp. 60–73.
15. Tilborg H. *Fundamentals of Cryptology: A Professional Reference and Interactive Tutorial*. London, Kluwer Academic Publishers, 2014. 414 p.
16. Dichenko S.A. Kontrol i obespechenie tselostnosti informatsii v sistemakh khraneniia dannykh [Control and Security of Information Integrity in Data Storage System]. *Naukoemkie tekhnologii v kosmicheskikh issledovaniakh Zemli* [High Technologies in Earth Space Research.], 2019, vol. 11, no. 1, pp. 49–57.
17. Dichenko S.A., Vishnevskii A.K., Finko O.A. Samoproveriaemyi spetsializirovannyi vychislitel sistem bulevykh funktsii [Self-Checking Special-Purpose Computer for Boolean Function Systems]. Pat. RF, no. 2485575. Date of filing: May 18, 2012. Date of Publ.: June 20, 2013. Bull. no. 17. 15 p.
- 18 Dichenko. S.A., Zharkikh A.A., Akilov A.A., Kis S.A. Razrabotka algoritma kontrolya i obespecheniya tselostnosti dannykh pri ikh khraneni v tsentrakh obrabotki dannykh [Algorithm Designing for Checking and Control the Integrity of Data during the Storage in Data Processing Centers]. *Informatsionnyi biulleten Omskogo nauchno-obrazovatel'nogo tsentra OmGTU i IM SO RAN v oblasti matematiki i informatiki. Mater. VIII Mezhdunar. molodezh. nauch.-prakt. konf. s elementami nauchnoi shkoly. Otv. red. A.V. Zykina* [News-Letter of Omsk Research-and-Education Center at Omsk State Technical University and the Sobolev Institute of Mathematics, RAS, in the Field of Mathematics and Informatics in Proc. of the 8th Int. Youth Sci. Workshop, A.V. Zykin (ed.)]. Omsk, 2018, pp. 110–113.
19. Finko O.A., Dichenko S.A. Two-dimensional Control and Assurance of Data Integrity in Information Systems Based on Residue Number System Codes and Cryptographic Hash Functions. *Proc. of the 2018 Multidisciplinary Symposium on Computer Science and ICT. October 15, 2018, 2254, CEUR Workshop Proceedings*. Stavropol, Russia, 2018, pp. 139–146.
20. Gardner M. *Neischerpaemoe ocharovanie treugolnika Paskalya. Matematicheskie novelly* [Mathematics Games. Pascal Pyramid]. Moscow, Mir Publ., 1974. 456 p.