МЕТОД ПАРАМЕТРИЧЕСКОГО СИНТЕЗА КРИПТО-КОДОВЫХ СТРУКТУР ДЛЯ КОНТРОЛЯ И ВОССТАНОВЛЕНИЯ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ

Диченко С.А.[1], Самойленко Д.В.[2], Финько О.А.[3], Рюмшин К.Ю.[4]

Цель *работы состоит в разработке метода контроля и восстановления целостности информации в защищённых многомерных системах хранения данных, обеспечивающего устойчивость рассматриваемых систем в условиях деструктивных воздействий злоумышленника и возмущений среды функционирования.*

Метод *исследования: в ходе проводимого исследования использовался научно-методический аппарат теории алгебраических систем в совокупности с методами криптографической защиты информации и математического аппарата теории кодирования для реализации процедур крипто-кодовых преобразований. Исследовались модели систем надёжного хранения данных для обоснования реализуемости процедур обеспечения подтверждённой целостности обрабатываемой информации.*

Результаты *исследования: способ формализованного представления информации в защищённых многомерных системах хранения данных, применяемых в интересах информационно-аналитических систем, позволяющий наглядного описать разработанные конструкции контроля и восстановления целостности данных в условиях деструктивных воздействий злоумышленника и возмущений среды функционирования. Представлена математическая модель процесса контроля и восстановления целостности данных на основе крипто-кодовых преобразований, основанных на агрегировании криптографических методов и методов помехоустойчивого кодирования. Комплексирование известных классических решений для обеспечения целостности данных позволит снизить вводимую избыточность, а также расширить функциональные возможности защищённых информационно-аналитических систем, заключающиеся в подтверждении достоверности восстановления целостности искажённых или утраченных данных без дополнительных затрат их повторного контроля криптографическими методами. Предложенная модель учитывает структуру многомерного представления информации в рассматриваемых системах хранения данных информационно-аналитических систем.*

Научная *новизна: разработанный метод параметрического синтеза крипто-кодовых структур для контроля и восстановления целостности информации в защищённых многомерных системах хранения данных отличается от известных получением оптимальных крипто-кодовых конструкций за счёт рационального агрегирования криптографических и кодовых преобразований в пространстве параметров рассматриваемых систем хранения данных. Формируемые на основе построения многомерных систем хэш-кодов и выполнения преобразований в расширенных полях Галуа крипто-кодовые конструкции обеспечивают криптографический контроль и восстановление целостности информации с возможностями гибкого введения избыточности и подтверждения с криптографической достоверностью целостности информации после процедуры восстановления.*

Вклад соавторов*: Диченко С.А. разработал математическую модель процесса контроля и восстановления целостности данных на основе крипто-кодовых преобразований, основанных на агрегировании криптографических методов и методов помехоустойчивого кодирования;*

Самойленко Д.В. разработал метод оценивания параметрического синтеза крипто-кодовых структур для контроля и восстановления целостности информации в защищённых многомерных системах хранения данных на основе совместного использования криптографических хэш-функций и модулярных полиномиальных кодов;

1 Диченко Сергей Александрович, кандидат технических наук, Краснодарское высшее военное училище им. генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: dichenko.sa@yandex.ru

2 Самойленко Дмитрий Владимирович, доктор технических наук, доцент, Краснодарское высшее военное училище им. генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: sam-0019@yandex.ru

3 Финько Олег Анатольевич, доктор технических наук, профессор, Краснодарское высшее военное училище им. генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: ofinko@yandex.ru

4 Рюмшин Константин Юрьевич, доктор технических наук, Московский технический университет связи и информатики, г. Москва, Россия. E-mail: e8@mail.ru

Финько О.А. разработал способы описания процесса контроля и восстановления целости данных в условиях деструктивных воздействий злоумышленника и возмущений среды функционирования;

Рюмшин К.Ю. разработал способ формализованного представления информации в защищённых многомерных системах хранения данных, применяемых в интересах информационно-аналитических систем.

Ключевые слова: *информационно-аналитические системы, Big Data, многомерное представление данных, подтверждённая целостность, криптографические методы, хэш-функция, помехоустойчивое кодирование, крипто-кодовые конструкции, эмерджентность.*

DOI:10.21681/2311-3456-2023-2-36-51

Введение

В соответствии со Стратегией развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года одним из приоритетных направлений исследований и разработок государства в области информационных технологий является обработка больших данных (Big Data). И как следствие одной из основных задач государства по развитию отрасли информационных технологий в этом направлении является развитие центров обработки и хранения информации как материальной основы для обработки и хранения больших массивов данных[5] [1].

Вопросам анализа больших массивов данных и извлечения знаний, включая новые методы и алгоритмы для сбора, хранения и интеллектуального анализа больших объемов данных; разработки новых способов хранения, обработки и передачи данных, включая новые устройства для хранения и обработки информации; создания новых высокопроизводительных систем вычислений и хранения данных, включая новые алгоритмы для высокопараллельных вычислений, посвящено достаточно много научных и практических работ [1 – 5]. При этом в современных условиях эволюционного роста объёма и ценности информации, обрабатываемой в информационных системах различного назначения, функционирующих в условиях деструктивных воздействий злоумышленника и среды, вопросы обеспечения их устойчивости оставались до последнего времени, по нашему мнению, без должного глубокого научного изучения. Среди немногих известны работы [6, 8], а также[6], в которых задача построения устойчивых информационных систем[7] решалась исключительно через обеспечение их живучести, надежности и помехоустойчивости, однако при этом вопросы безопасности информации, обрабатываемой в информационных системах или хранящейся в подсистемах хранения, остаются без должного внимания.

Необходимо отдельно обозначить актуальность такой прикладной области как развитие защищённых информационно-аналитических систем (далее – ИАС), в которых обрабатывается специальная информация, достоверность которой играет особую роль. В условиях деструктивных воздействий одним из основных требований, предъявляемых к системам хранения данных (далее – СХД), как основному сегменту ИАС, напрямую связанного с правильностью принимаемого пользователем системы решения, является обеспечение защищённости хранящейся в них информации, в частности, обеспечение её целостности (рис. 1).

Наиболее популярным из существующих решений является комплексное обеспечение целостности данных, где, к сожалению, задачи контроля и восстановления целостности данных решаются раздельно: для контроля целостности данных применяются методы из области безопасности информации (криптографические преобразования), а для восстановления целостности — методы теории надёжности (технология резервного копирования), что, как известно, достигается ценой высокой избыточности. К тому же выстроенная последовательность решения задач контроля, а затем, в случае обнаружения ошибки, восстановления целостности данных приводит к отсутствию возможности подтверждения с криптографической стойкостью достоверности утраченных или искажённых данных,

5 Стратегией развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года (утв. распоряжением Правительства РФ от 1 ноября 2013 г. № 2036-р).

6 Басыров А.Г., Захаров И.В. Оценивание живучести бортовых вычислительных систем космических аппаратов // Труды Военно-космической академии имени А.Ф. Можайского. 2016. №651. С. 139 – 148.

7 Флешман Б.С. Основы системологии // М.: Радио и связь. 1982. – 368 с.

Рис. 1. Устойчивость ИАС через свойство безопасности информации

что является критичным для защищённых ИАС, в которых обрабатывается специальная информация.

Формализованное представление данных в защищённых информационно-аналитических системах для описания крипто-кодовых конструкций контроля и восстановления их целостности

Защищённые ИАС характеризуются обработкой больших многомерных массивов информации в условиях деструктивных воздействий злоумышленника и среды. Для таких условий функционирования одной из актуальнейших задач является организация безопасного хранения данных, обеспечивающая их тождественность у оператора, отправившего данные на хранение, и у лица, принимающего решение, при запросе на их использование.

Одной из особенностей защищённых ИАС является то, что для них наряду с информационными системами другого назначения критичным является время получения ответов на запросы пользователей системы. Поэтому для ИАС характерно представление информации не в виде реляционных таблиц, а в виде упорядоченных многомерных массивов информации. Многомерная модель данных, лежащая в основе построения современных СХД защищённых ИАС, опирается на концепцию многомерных кубов или гиперкубов (рис. 2).

В процессе поиска и извлечения из гиперкуба необходимой информации над его измерениями производится ряд действий, наиболее типичными из которых являются: сечение (срез); транспонирование; свёртка; детализация.

Для декомпозиции многомерного массива информации, хранящейся в СХД защищённых ИАС, используя известные правила, выполняется его расчленение на сечения (сечения гиперкуба данных), которое заключается в выделении подмножества ячеек гиперкуба при фиксировании значения одного или нескольких измерений.

В результате расчленения на сечения получается срез или несколько срезов, каждый из которых содержит информацию, связанную со значением измерения, по которому он был построен.

Формализованное представление данных в 1-мерном пространстве

При фиксировании двух произвольных измерений на одном из срезов гиперкуба данных получим множество ячеек – блоков данных, которые обозначим как M_i блоки, полученные посредством декомпозиции гиперкуба8 данных M, где $i = 1,2,\dots,k$ (рис. 3).

Данные в 1-мерном пространстве также можно представить путём фиксирования по одному отличному друг от друга измерению на разных срезах гиперкуба данных, при этом получим два пересекающихся в пространстве сечения, содержащие в себе множество ячеек – блоков данных, которые также обозначим как M_i блоки (рис. 4).

Полученные блоки данных, с одной стороны, могут интерпретироваться как двоичные числа: $M_i = (\mu_{t-1} \dots \mu_1 \mu_0)_2$, где $\mu_g \in \{0,1\}$; $g = 0,1,\dots,t-1$, или десятичные: $M_i = \mu_0 + 2\mu_1 + \dots + 2^{t-1}\mu_{t-1}$, где $M_i \in N$. С другой стороны, полученные блоки дан-

8 Тарасов С.В. СУБД для программиста. Базы данных изнутри. – М.: СОЛОН-Пресс. 2015. – 320 с.

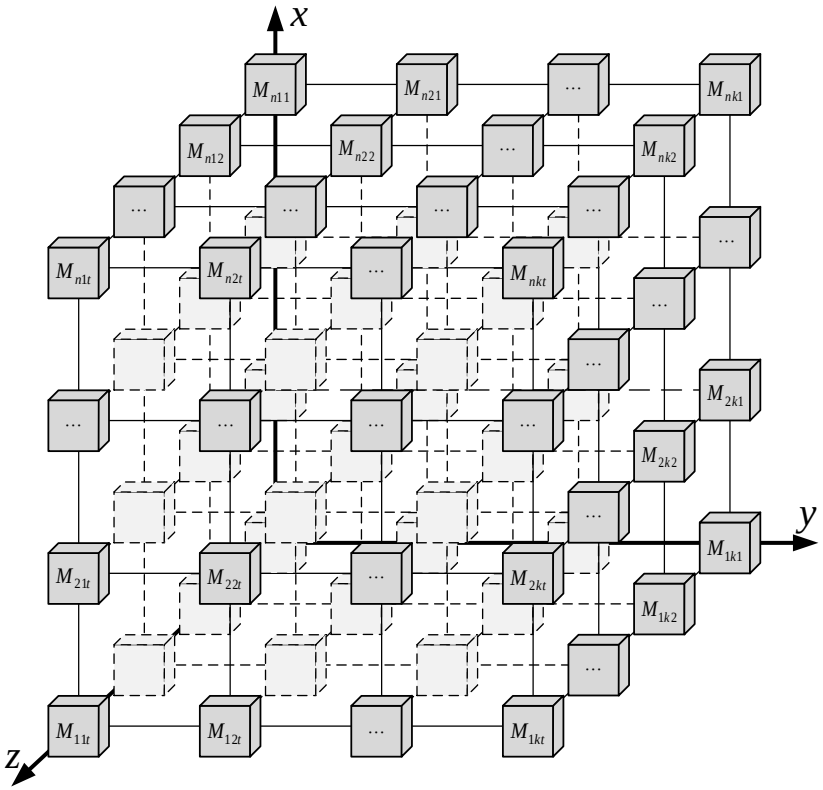


Рис. 2. Принцип организации многомерного куба данных

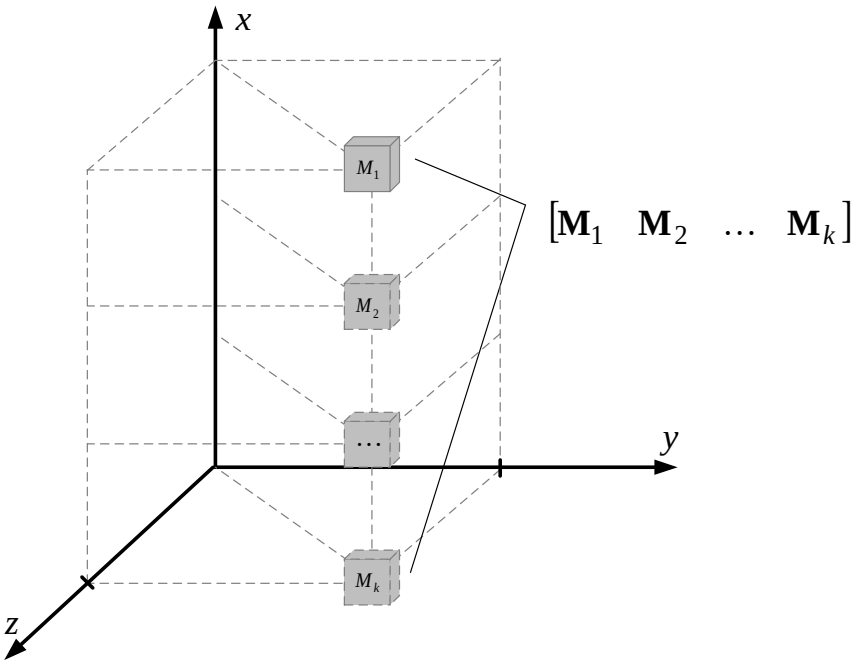


Рис. 3. Представление данных в 1-мерном пространстве

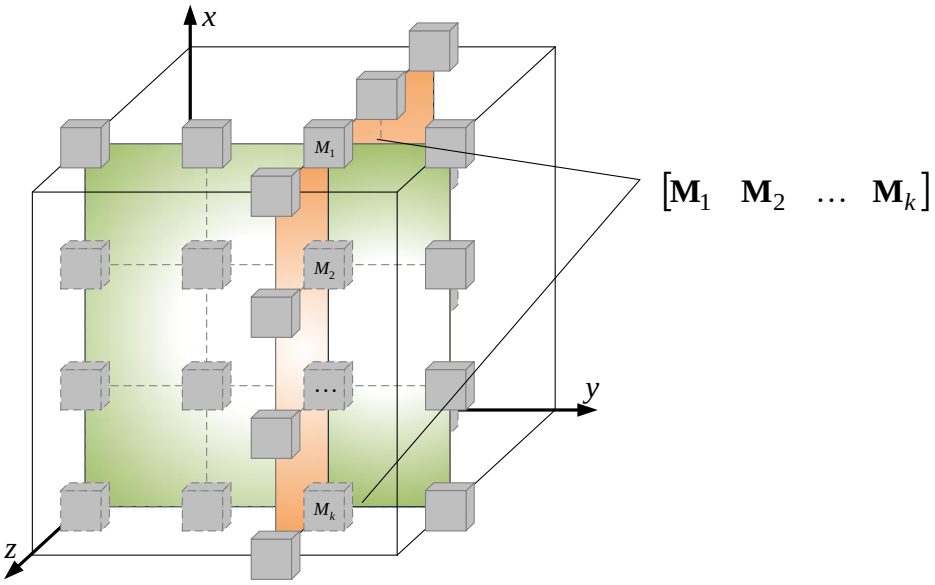


Рис. 4. Представление данных в 1-мерном пространстве на пересечении двух срезов гиперкуба данных

ных M_i могут быть представлены в полиномиальной форме:
$M_i(z) = \sum_{g=0}^{t-1} \mu_g z^g = \mu_{t-1} z^{t-1} + \mu_{t-2} z^{t-2} + \cdots + \mu_0$,
где $\mu_g \in \{0,1\}$; $g = t-1, t-2, \ldots, 0$.

Также блоки данных M_i могут рассматриваться как двоичные векторы $\boldsymbol{M}_i$: $\boldsymbol{M}_i = [\mu_1 \quad \mu_2 \quad \ldots \quad \mu_t]$, где $\mu_g \in \{0,1\}$; $g = 1,2,\ldots,t$.

Декомпозиция гиперкуба данных M представлена следующим выражением: $\mathrm{Frag}(M) = [\boldsymbol{M}_1 || \boldsymbol{M}_2 || \ldots || \boldsymbol{M}_k]$, где $\mathrm{Frag}(M)$ – операция фрагментации, «||» – операция конкатенации (объединения).

В результате получим вектор $\boldsymbol{\Omega}$:

$$\boldsymbol{\Omega} = [\boldsymbol{M}_1 \quad \boldsymbol{M}_2 \quad \ldots \quad \boldsymbol{M}_k], \qquad (1)$$

где $\boldsymbol{\Omega}$ – вектор векторов $\boldsymbol{M}_1, \boldsymbol{M}_2, \ldots, \boldsymbol{M}_k$.

Формализованное представление данных в 2-мерном пространстве

В случае фиксирования одного измерения (рис. 5) получим сечение гиперкуба данных, содержащее в себе множество ячеек – блоков данных M_{ij}, где $i = 1,2,\ldots,n$; $j = 1,2,\ldots,k$.

Полученные блоки данных, с одной стороны, могут интерпретироваться как двоичные числа: $M_{ij} = \left(\mu_{t-1}^{(ij)} \ldots \mu_1^{(ij)} \mu_0^{(ij)}\right)_2$, где $\mu_g^{(ij)} \in \{0,1\}$; $g = 0,1,\ldots,t-1$, или десятичные: $M_{ij} = \mu_0^{(ij)} + 2\mu_1^{(ij)} + \cdots + 2^{t-1}\mu_{t-1}^{(ij)}$, где $M_{ij} \in N$. С другой стороны, полученные блоки данных M_{ij} могут быть представлены в полиномиальной форме:

$$M_{ij}(z) = \sum_{g=0}^{t-1} \mu_g^{(ij)} z^g = \mu_{t-1}^{(ij)} z^{t-1} + \mu_{t-2}^{(ij)} z^{t-2} + \cdots + \mu_0^{(ij)},$$

где $\mu_g^{(ij)} \in \{0,1\}$; $g = t-1, t-2, \ldots, 0$.

К тому же блоки данных M_{ij} могут рассматриваться как двоичные векторы $\boldsymbol{M}_{ij}$: $\boldsymbol{M}_{ij} = \left[\mu_1^{(ij)} \quad \mu_2^{(ij)} \quad \ldots \quad \mu_t^{(ij)}\right]$, где $\mu_g^{(ij)} \in \{0,1\}$; $g = 1,2,\ldots,t$.

При этом декомпозиция гиперкуба данных M представлена следующим выражением:

$$\mathrm{Frag}(M) = [\boldsymbol{M}_{11} || \ldots || \boldsymbol{M}_{1k} || \boldsymbol{M}_{21} || \ldots || \boldsymbol{M}_{2k} || \ldots || \boldsymbol{M}_{n1} || \ldots || \boldsymbol{M}_{nk}].$$

В результате декомпозиция получим двумерную матрицу $\boldsymbol{\Psi}$, имеющую n строк и k столбцов:

$$\boldsymbol{\Psi} = \begin{bmatrix} \boldsymbol{M}_{11} & \boldsymbol{M}_{12} & \ldots & \boldsymbol{M}_{1k} \\ \boldsymbol{M}_{21} & \boldsymbol{M}_{22} & \ldots & \boldsymbol{M}_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{M}_{n1} & \boldsymbol{M}_{n2} & \ldots & \boldsymbol{M}_{nk} \end{bmatrix}. \qquad (2)$$

Матрицу (2) можно также получить путём заполнения произвольной матрицы векторами векторов $\boldsymbol{M}_{i1}, \boldsymbol{M}_{i2}, \ldots, \boldsymbol{M}_{ik}$ вида (1).

Сокращённая запись матрицы (2) будет иметь вид:

$$\boldsymbol{\Psi} = [\boldsymbol{M}_{ij}] \text{ или } \boldsymbol{\Psi} = [\boldsymbol{M}_{ij}]_{n \times k}.$$

Нумерация блоков данных на (рис. 3 – 5) выполнена независимо от начала системы координат. Это сделано для удобства и стремления приведения формы математического обозначения блоков данных,

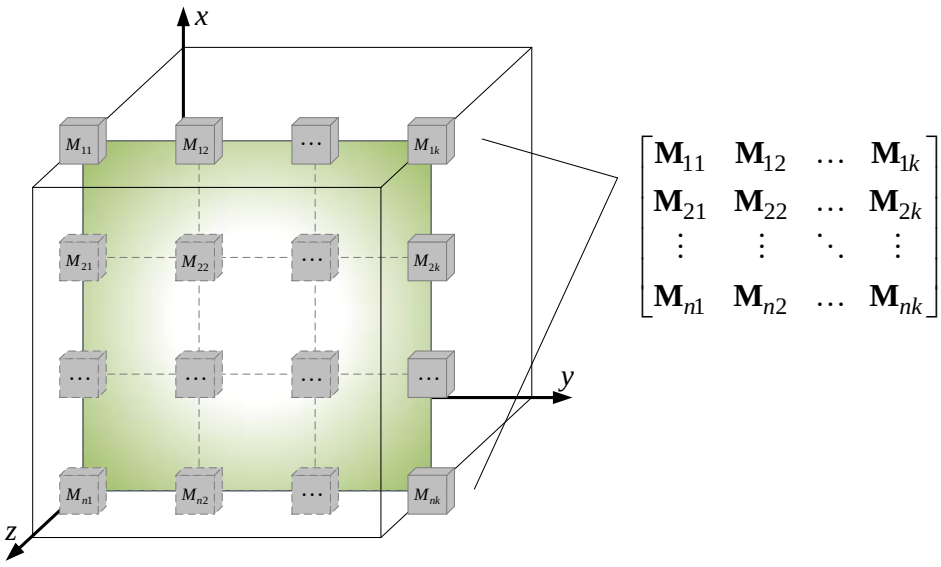


Рис. 5. Представление данных в 2-мерном пространстве

представленных в 1- и 2-мерном пространстве, к привычному виду, где нумерация элементов вектора осуществляется слева направо (строк матрицы — слева направо, столбцов – сверху вниз).

Формализованное представление данных в *n*-мерном пространстве

В соответствии с теорией многомерных матриц9 данные, хранящиеся в многомерном кубе, также могут быть представлены P-мерной матрицей (многомерной матрицей), под которой понимается совокупность элементов $C_{i_1 \dots i_p}$, где индексы $i_1 \dots i_p$ принимают значения от 1 до n_a соответственно, где $a = 1, \dots, p$.

P-мерная матрица содержит $n_1 \times n_2 \times \dots \times n_p$ элементов и обозначается как $\boldsymbol{C}_M = \left[c_{i_1 \dots i_p}\right]$.

При этом многомерный куб данных можно рассматривать как систему координат с осями, например, для трёхмерного куба (частный случай, рис. 2): x, y, z, по которым откладываются блоки данных.

К примеру, при фиксировании значений по оси x (частный случай: $x = 1$) получим:

$$\begin{bmatrix} \boldsymbol{M}_{111} & \boldsymbol{M}_{112} & \dots & \boldsymbol{M}_{11t} \\ \boldsymbol{M}_{121} & \boldsymbol{M}_{122} & \dots & \boldsymbol{M}_{12t} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{M}_{1k1} & \boldsymbol{M}_{1k2} & \dots & \boldsymbol{M}_{1kt} \end{bmatrix}.$$

В такой системе каждому блоку данных M_{ijr} ($i = 1,2,\dots,n;\ j = 1,2,\dots,k;\ r = 1,2,\dots,t$), хранящемуся в СХД ИАС, соответствует определенная ячейка, в которой размещается его содержимое.

В классических OLAP-кубах, содержимое называется числовыми показателями (фактами), связанными с данным набором. Таким образом, между объектами и их числовыми характеристиками устанавливается однозначная связь.

Таким образом, информация в СХД защищённых ИАС будет являться логически целостной. Это уже не просто наборы строковых и числовых значений, которые в случае реляционной модели нужно получать из различных таблиц, а целостные структуры с однозначными связями, что делает преимущества многомерного подхода очевидными. Формализованное представление данных в виде (1) или (2) позволит описать конструкции контроля и восстановления их целостности в условиях деструктивных воздействий.

Математическая модель процесса контроля и восстановления целостности данных для защищённых информационно-аналитических систем на основе крипто-кодовых преобразований

В настоящее время для обеспечения целостности данных в СХД защищённых ИАС применяются различные решения, объединяемые одной общей характерной чертой, заключающейся в последовательном применении для контроля целостности данных методов из области безопасности информации, к примеру, функцию хэширования, а для восстановления целостности данных — методов теории надёжности (наиболее популярной является технология резервного копиро-

9 Соколов Н.П. Введение в теорию многомерных матриц – М.: Просвещение. 2012. –175 с.

вания), что, как известно [10, 11], достигается ценой высокой избыточности[10].

К тому же в условиях деструктивных воздействий злоумышленника и среды общепринятая последовательность решения задач сначала контроля, а затем, в случае обнаружения ошибки, восстановления целостности данных приводит к невозможности подтверждения правильности восстановления целостности искажённых или утраченных данных, так как данная процедура может выполняться исключительно с заданной вероятностью [12], что является критичным для защищённых ИАС, в которых обрабатывается специальная информация.

Для обеспечения возможности совместного контроля и восстановления целостности данных предлагается построение крипто-кодовых конструкций [13 – 17], применение которых позволит исключить недостатки известных решений.

Правила построения крипто-кодовых конструкций будут определяться посредством φ -функции («фи-функции»), под которой будем понимать функцию, отображающую совокупность данных X и Y, в дополнительные данные Z:

$$\varphi^{(nD)}(X,Y) \to Z,$$

где nD — мерность пространства, в котором выполняются преобразования (зависит от модели представления данных в СХД), к примеру, выражение: $n = 1,2,3,\ldots$ обозначает 1-, 2-, 3-мерное пространство соответственно; X и Y — аргументы φ-функции, являющиеся результатами разных типов преобразований, при этом данные X будут использоваться для осуществления контроля целостности данных, подлежащих защите, а данные Y — для возможности последующего восстановления целостности в случае её нарушения.

Пример 1. Если за аргументы φ-функции X, Y принять значения функций кодирования $f(M)$ и хэширования $h(M)$ соответственно, то φ-функцию можно представить, как

$$\varphi^{(nD)}\left(f(M),h(M)\right) \to Z,$$

где M — произвольный блок данных, подлежащий защите.

Значения функций кодирования $X = f(M)$ и хэширования $Y = h(M)$ будем считать контрольными символами, используемыми для осуществления контроля и восстановления целостности данных, а значение φ -функции Z — дополнительными контрольными символами, используемые при комплексном обеспечении целостности блока данных M, подлежащего защите, заключающемся в дополнительном подтверждении правильности восстановления целостности искажённых или утраченных данных.

Пример 2. В 2-мерном пространстве под φ -функцией понимается функция, отображающая совокупность данных, представленных двоичными векторами $\boldsymbol{X}_{i\upsilon}$ и $\boldsymbol{Y}_{\vartheta j}$, в дополнительные данные $\boldsymbol{Z}_{\vartheta\upsilon}$: $\varphi^{(2D)}\left(\boldsymbol{X}_{i\upsilon},\boldsymbol{Y}_{\vartheta j}\right) \to \boldsymbol{Z}_{\vartheta\upsilon}$, где $\boldsymbol{X}_{i\upsilon}$, $\boldsymbol{Y}_{\vartheta j}$ — контрольные символы, полученные в результате преобразований над данными, представленных $\boldsymbol{M}_{ij}$ блоками; $\boldsymbol{Z}_{\vartheta\upsilon}$ — дополнительные контрольные символы.

Получим матрицу $\boldsymbol{\Psi}$:

$$\boldsymbol{\Psi} = \left[\begin{array}{cccc|ccc} \mathbf{M}_{11} & \mathbf{M}_{12} & \ldots & \mathbf{M}_{1k} & \mathbf{X}_{11} & \ldots & \mathbf{X}_{1v} \\ \mathbf{M}_{21} & \mathbf{M}_{22} & \ldots & \mathbf{M}_{2k} & \mathbf{X}_{21} & \ldots & \mathbf{X}_{2v} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{M}_{n1} & \mathbf{M}_{n2} & \ldots & \mathbf{M}_{nk} & \mathbf{X}_{n1} & \ldots & \mathbf{X}_{nv} \\ \hline \mathbf{Y}_{11} & \mathbf{Y}_{12} & \ldots & \mathbf{Y}_{1k} & \mathbf{Z}_{11} & \ldots & \mathbf{Z}_{1v} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{Y}_{u1} & \mathbf{Y}_{u2} & \ldots & \mathbf{Y}_{uk} & \mathbf{Z}_{u1} & \ldots & \mathbf{Z}_{uv} \end{array}\right], \quad (3)$$

где $\boldsymbol{X}_{i\upsilon}$, $\boldsymbol{Y}_{\vartheta j}$ и $\boldsymbol{Z}_{\vartheta\upsilon}$ – двоичные векторы, являющиеся элементами матрицы (3), образующие подматрицы $[\boldsymbol{X}_{i\upsilon}]$, $[\boldsymbol{Y}_{\vartheta j}]$ и $[\boldsymbol{Z}_{\vartheta\upsilon}]$; $i = 1,2,\ldots,n$; $\upsilon = 1,2,\ldots,v$; $j = 1,2,\ldots,k$; $\vartheta = 1,2,\ldots,u$.

Приняв за аргументы φ-функции результаты вычислений функций кодирования $f(\boldsymbol{M}_{ij})$ и хэширования $h(\boldsymbol{M}_{ij})$, φ -функцию можно представить следующим выражением: $\varphi^{(2D)}\left(f(\boldsymbol{M}_{ij}),h(\boldsymbol{M}_{ij})\right)$.

Здесь аргументами φ-функции являются значения функций кодирования $f(\boldsymbol{M}_{ij})$ и хэширования $h(\boldsymbol{M}_{ij})$, которые условно будем считать контрольными символами $\boldsymbol{X}_{i\upsilon}$ и $\boldsymbol{Y}_{\vartheta j}$ соответственно.

Сокращённая запись матрицы (3) будет иметь вид:

$$\boldsymbol{\Psi} = \left[\begin{array}{c|c} \mathbf{M}_{ij} & \mathbf{X}_{i\upsilon} \\ \hline \mathbf{Y}_{\vartheta j} & \mathbf{Z}_{\vartheta\upsilon} \end{array}\right],$$

где $\boldsymbol{Z}_{\vartheta\upsilon}$ – элемент матрицы $\boldsymbol{\Psi}$, являющийся результатом вычисления φ-функции.

Представленная модель учитывает структуру многомерного представления информации в современных СХД. Агрегирование известных классических решений для обеспечения целостности данных позволит снизить вводимую избыточность, а также расширить функциональные возможности защищённых ИАС, за-

10 Schneier B. Applied Cryptography Second Edition: protocols, algorithms and source code in C. – John Wiley & Sons. 2016. – 653 p.

ключающееся в подтверждении правильности восстановления целостности искажённых или утраченных данных за счёт возможности без дополнительных затрат их повторного контроля криптографическими методами.

Метод параметрического синтеза крипто-кодовых структур для контроля и восстановления целостности информации в защищённых многомерных системах хранения данных

Метод синтеза контроля и восстановления целостности данных, представленных в виде упорядоченных многомерных массивов (гиперкубов), основан на совместном использовании криптографических методов (функции хэширования) и методов помехоустойчивого кодирования (избыточных МПК).

Путем фиксации одного из измерений гиперкуба данных получим матрицу $\boldsymbol{W}$, на строках и столбцах которой располагаются подблоки данных M_{ij}, подлежащие защите:

$$\boldsymbol{W} = \begin{bmatrix} M_{11} & M_{12} & \cdots & M_{1n} \\ M_{21} & M_{22} & \cdots & M_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ M_{n1} & M_{n2} & \cdots & M_{nn} \end{bmatrix}. \quad (4)$$

При этом строки матрицы (4) образуют блоки данных $M_i = \{M_{i1} \| M_{i2} \| \ldots \| M_{in}\}$, столбцы матрицы – блоки данных $M_j = \{M_{1j} \| M_{2j} \| \ldots \| M_{nj}\}$, где $i, j = 1,2,\ldots,n$.Для контроля целостности данных, подлежащих защите, к блокам данных M_i, которые интерпретируются как двоичные векторы $\boldsymbol{M}_i$, применим хэш-функцию.

Полученные хэш-коды $\boldsymbol{H}_i$ хэш-функции $h(\boldsymbol{M}_i)$ (или $h_k(\boldsymbol{M}_i)$, где k — секретный ключ) от блоков данных $\boldsymbol{M}_i$ будут являться эталонными:

$$\boldsymbol{\Psi} = \left[\begin{bmatrix} \boldsymbol{M}_{11} & \boldsymbol{M}_{12} & \cdots & \boldsymbol{M}_{1n} \\ \boldsymbol{M}_{21} & \boldsymbol{M}_{22} & \cdots & \boldsymbol{M}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{M}_{n1} & \boldsymbol{M}_{n2} & \cdots & \boldsymbol{M}_{nn} \end{bmatrix} \begin{matrix} \to \\ \to \\ \vdots \\ \to \end{matrix} \right.$$

$$\left. \begin{matrix} \to \\ \to \\ \vdots \\ \to \end{matrix} \begin{bmatrix} \boldsymbol{H}_{11} & \boldsymbol{H}_{12} & \cdots & \boldsymbol{H}_{1n} \\ \boldsymbol{H}_{21} & \boldsymbol{H}_{22} & \cdots & \boldsymbol{H}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{H}_{n1} & \boldsymbol{H}_{n2} & \cdots & \boldsymbol{H}_{nn} \end{bmatrix} \right],$$

где $\boldsymbol{H}_i = \{\boldsymbol{H}_{i1} \| \boldsymbol{H}_{i2} \| \ldots \| \boldsymbol{H}_{in}\}$.

В свою очередь, для возможности восстановления целостности данных, подлежащих защите, подблоки M_{ij} блоков данных M_j представим в полиномиальной форме:

$$M_{ij}(z) = \sum_{g=0}^{t-1} \mu_g^{(ij)} z^g = \mu_{t-1}^{(ij)} z^{t-1} + \mu_{t-2}^{(ij)} z^{t-2} + \cdots + \mu_0^{(ij)},$$

где $\mu_g^{(ij)} \in \{0,1\}; g = t-1, t-2, \ldots, 0$.

Полученные подблоки $M_{ij}(z)$ блоков данных M_j, представленные в полиномиальной форме, интерпретируются как наименьшие неотрицательные вычеты по основаниям $p_{ij}(z)$ таким, что $gcd\left(p_{i_1 j}(z), p_{i_2 j}(z)\right) = 1$, где $i_1 \neq i_2, i_1, i_2 = 1,2,\ldots,n$.

При этом

$$deg\, M_{ij}(z) < deg\, p_{ij}(z)$$

где $deg\, M_{ij}(z)$ – степень полинома $M_{ij}(z)$.

Далее совокупность подблоков $M_{1j}(z), M_{2j}(z), \ldots, M_{nj}(z)$ блока данных M_j представим как единый суперблок МПК по системе оснований $p_{1j}(z), p_{2j}(z), \ldots, p_{nj}(z)$.

В соответствии с Китайской теоремой об остатках для многочленов для заданного множества многочленов $p_{1j}(z), p_{2j}(z), \ldots, p_{nj}(z)$, удовлетворяющих условию $gcd\left(p_{i_1 j}(z), p_{i_2 j}(z)\right) = 1$, и многочленов $M_{1j}(z), M_{2j}(z), \ldots, M_{nj}(z)$ таких, что $deg\, M_{ij}(z) < deg\, p_{ij}(z)$, система сравнений

$$\begin{cases} X(z) \equiv M_{1j}(z) \mod p_{1j}(z), \\ X(z) \equiv M_{2j}(z) \mod p_{2j}(z), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X(z) \equiv M_{nj}(z) \mod p_{nj}(z) \end{cases} \quad (5)$$

имеет единственное решение $X(z)$ [18].

Выполним операцию расширения МПК $\{M_{1j}(z), M_{2j}(z), \ldots, M_{nj}(z)\}_{\text{МПК}}$ путём введения $k-n$ избыточных оснований $p_{n+1,j}(z), p_{n+2,j}(z), \ldots, p_{k,j}(z)$ и получим избыточные вычеты $M_{n+1,j}(z), M_{n+2,j}(z), \ldots, M_{kj}(z)$:

$$\begin{cases} M_{n+1,j}(z) \equiv X(z) \mod p_{n+1,j}(z), \\ M_{n+2,j}(z) \equiv X(z) \mod p_{n+2,j}(z), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ M_{kj}(z) \equiv X(z) \mod p_{kj}(z). \end{cases}$$

Причём

$$\gcd\left(p_{i_1 j}(z), p_{i_2 j}(z)\right) = 1,$$

где $deg\, p_{1j}(z), \ldots, deg\, p_{nj}(z) < deg\, p_{n+1,j}(z) < \cdots$ $\cdots < deg\, p_{kj}(z), i_1, i_2 = 1,2,\ldots,k, i_1 \neq i_2$.

Получим расширенный МПК в кольце многочленов: $\{M_{1j}(z), M_{2j}(z), \ldots, M_{nj}(z), M_{n+1,j}(z), M_{n+2,j}(z), \ldots, M_{kj}(z)\}_{\text{МПК}}$

и матрицу $\boldsymbol{Y}$:

$$\boldsymbol{Y} = \left[\begin{bmatrix} M_{11}(z) & M_{12}(z) & \cdots & M_{1n}(z) \\ M_{21}(z) & M_{22}(z) & \cdots & M_{2n}(z) \\ \vdots & \vdots & \ddots & \vdots \\ M_{n1}(z) & M_{n2}(z) & \cdots & M_{nn}(z) \end{bmatrix} \right.$$

$$\left. \begin{matrix} \downarrow & \downarrow & \cdots & \downarrow \end{matrix} \begin{bmatrix} M_{n+1,1}(z) & M_{n+1,2}(z) & \cdots & M_{n+1,n}(z) \\ M_{n+2,1}(z) & M_{n+2,2}(z) & \cdots & M_{n+2,n}(z) \\ \vdots & \vdots & \ddots & \vdots \\ M_{k1}(z) & M_{k2}(z) & \cdots & M_{kn}(z) \end{bmatrix} \right].$$

Для выполнения операций между полученными j -ми избыточными подблоками блоков данных M_j и i -ми подблоками хэш-кодов, выраженными двоичными векторами $\boldsymbol{H}_i$, выполним обратное сопоставление многочленов:
$M_{1j}(z), M_{2j}(z), \dots, M_{nj}(z), M_{n+1,j}(z), M_{n+2,j}(z), \dots, M_{kj}(z)$
их двоичным векторам:

$$M_{\xi j}(z) = \mu_{t-1}^{(\xi j)} z^{t-1} + \dots + \mu_0^{(\xi j)} \Rightarrow$$
$$\Rightarrow \quad \boldsymbol{M}_{\xi j} = \left[\mu_{t-1}^{(\xi j)} \quad \dots \quad \mu_0^{(\xi j)}\right],$$

где $\xi = 1,2,\dots,n,n+1,n+2,\dots,k$.

Получим матрицу $\boldsymbol{\Xi}$:

$$\boldsymbol{\Xi} = \left[\begin{array}{cccc|ccc} \mathbf{M}_{11} & \mathbf{M}_{12} & \dots & \mathbf{M}_{1n} & \mathbf{H}_{11} & \dots & \mathbf{H}_{1n} \\ \mathbf{M}_{21} & \mathbf{M}_{22} & \dots & \mathbf{M}_{2n} & \mathbf{H}_{21} & \dots & \mathbf{H}_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{M}_{n1} & \mathbf{M}_{n2} & \dots & \mathbf{M}_{nn} & \mathbf{H}_{n1} & \dots & \mathbf{H}_{nn} \\ \hline \mathbf{M}_{n+1,1} & \mathbf{M}_{n+1,2} & \dots & \mathbf{M}_{n+1,n} & & & \\ \vdots & \vdots & \ddots & \vdots & & & \\ \mathbf{M}_{k1} & \mathbf{M}_{k2} & \dots & \mathbf{M}_{kn} & & & \end{array}\right].$$

Выполним сложение i -х подблоков хэш-кодов $\boldsymbol{H}_i$ с j -ми избыточными подблоками блоков данных $\boldsymbol{M}_j$ кодового вектора МПК:

$$\boldsymbol{G}_i = \boldsymbol{H}_i \oplus \boldsymbol{M}_j = [\boldsymbol{H}_{i1} \oplus \boldsymbol{M}_{n+1,j} \quad \boldsymbol{H}_{i2} \oplus \boldsymbol{M}_{n+2,j} \quad \dots$$
$$\dots \quad \boldsymbol{H}_{in} \oplus \boldsymbol{M}_{kj}],$$

где «$\oplus$» — символ сложения в $GF(2)$, $\boldsymbol{G}_i = [\boldsymbol{G}_{i1} \quad \boldsymbol{G}_{i2} \quad \dots \quad \boldsymbol{G}_{in}]$; $\boldsymbol{H}_i = [\boldsymbol{H}_{i1} \quad \boldsymbol{H}_{i2} \quad \dots \quad \boldsymbol{H}_{in}]$; $\boldsymbol{M}_j = [\boldsymbol{M}_{n+1,j} \quad \boldsymbol{M}_{n+2,j} \quad \dots \quad \boldsymbol{M}_{kj}]$.

Получим матрицу:

$$\boldsymbol{\Omega} = \left[\begin{bmatrix} \boldsymbol{M}_{11} & \boldsymbol{M}_{12} & \cdots & \boldsymbol{M}_{1n} \\ \boldsymbol{M}_{21} & \boldsymbol{M}_{22} & \cdots & \boldsymbol{M}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{M}_{n1} & \boldsymbol{M}_{n2} & \cdots & \boldsymbol{M}_{nn} \end{bmatrix} \begin{bmatrix} \boldsymbol{G}_{11} & \boldsymbol{G}_{12} & \cdots & \boldsymbol{G}_{1n} \\ \boldsymbol{G}_{21} & \boldsymbol{G}_{22} & \cdots & \boldsymbol{G}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{G}_{n1} & \boldsymbol{G}_{n2} & \cdots & \boldsymbol{G}_{nn} \end{bmatrix}\right]. \quad (6)$$

Данные, подлежащие защите, представленные в виде (6) могут быть отправлены на хранение.

При запросе на использование защищаемых данных M_{ij}, представленных в виде (6), сначала выполняется контроль их целостности, для этого сопоставим двоичные векторы $\boldsymbol{M}_{ij}$ их многочленам:

$$\boldsymbol{M}_{\varsigma j} = \left[\mu_{t-1}^{(\varsigma j)} \quad \dots \quad \mu_0^{(\varsigma j)}\right] \Rightarrow$$
$$\Rightarrow \quad M_{\varsigma j}(z) = \mu_{t-1}^{(\varsigma j)} z^{t-1} + \dots + \mu_0^{(\varsigma j)},$$

где $\varsigma = 1,2,\dots,n$.

Выполним операцию расширения информационного суперблока МПК, в результате которой формируются избыточные подблоки $M'_{n+1,j}(z), M'_{n+2,j}(z), \dots, M'_{kj}(z)$ блоков данных M'_j, где символ «$(\cdot)'$» обозначает, что могло произойти нарушение целостности данных M'_{ij}, находящихся на хранении, представленных подблоками $M_{1,j}(z), M_{2,j}(z), \dots, M_{nj}(z)$[11]

Получим матрицу с избыточными подблоками кодового вектора МПК:

$$\boldsymbol{\Omega}' = \left[\begin{bmatrix} M'_{11}(z) & M'_{12}(z) & \cdots & M'_{1n}(z) \\ M'_{21}(z) & M'_{22}(z) & \cdots & M'_{2n}(z) \\ \vdots & \vdots & \ddots & \vdots \\ M'_{n1}(z) & M'_{n2}(z) & \cdots & M'_{nn}(z) \end{bmatrix} \downarrow \quad \downarrow \quad \cdots \quad \downarrow \begin{bmatrix} M'_{n+1,1}(z) & M'_{n+1,2}(z) & \cdots & M'_{n+1,n}(z) \\ M'_{n+2,1}(z) & M'_{n+2,2}(z) & \cdots & M'_{n+2,n}(z) \\ \vdots & \vdots & \ddots & \vdots \\ M'_{k1}(z) & M'_{k2}(z) & \cdots & M'_{kn}(z) \end{bmatrix}\right].$$

Выполним обратное сопоставление многочленов $M'_{n+1,j}(z), M'_{n+2,j}(z), \dots, M'_{kj}(z)$ их двоичным векторам[12]:

$$M'_{\varsigma j}(z) = \mu_{t-1}^{(\varsigma j)} z^{t-1} + \dots + \mu_0^{(\varsigma j)} \Rightarrow$$
$$\Rightarrow \quad \boldsymbol{M}'_{\varsigma j} = \left[\mu_{t-1}^{(\varsigma j)} \quad \dots \quad \mu_0^{(\varsigma j)}\right],$$

где $\varsigma = n+1,n+2,\dots,k$.

Выполним обратные преобразования:

$$\boldsymbol{H}'_i = \boldsymbol{G}_i \oplus \boldsymbol{M}'_j = \left[\boldsymbol{G}_{i1} \oplus \boldsymbol{M}'_{n+1,j} \quad \boldsymbol{G}_{i2} \oplus \boldsymbol{M}'_{n+2,j} \quad \dots\right.$$
$$\left. \dots \quad \boldsymbol{G}_{in} \oplus \boldsymbol{M}'_{kj}\right].$$

Сравним значения полученных хэш-кодов $\boldsymbol{H}'_i$ со значениями ранее вычисленных эталонных хэш-кодов $\boldsymbol{H}_i$, хранящиеся в надежной среде, а также хэш-кодов $\boldsymbol{H}''_i$, вычисленных посредством хэш-функции $h(\boldsymbol{M}'_i)$. По результатам сравнения сделаем вывод об отсутствии нарушения целостности данных, при $\boldsymbol{H}'_i = \boldsymbol{H}_i$ и $\boldsymbol{H}'_i = \boldsymbol{H}''_i$; либо о нарушении целостности данных, при $\boldsymbol{H}'_i \neq \boldsymbol{H}_i$ и $\boldsymbol{H}'_i \neq \boldsymbol{H}''_i$.

Таким образом, определение факта нарушения целостности подблока данных M'_{ij}, находящихся на хранении, посредством сравнения хэш-кодов, будет являться локализацией по строкам матрицы блока $\widetilde{\boldsymbol{M}}_i$ с нарушением целостности входящего в него подблока $\widetilde{\boldsymbol{M}}_{ij}$ (в случае однократной ошибки) или нескольких подблоков.

Затем посредством математического аппарата МПК выполняется локализация одного или нескольких подблоков $\widetilde{\boldsymbol{M}}_{ij}$, входящих в блок данных $\widetilde{\boldsymbol{M}}_j$, по столбцам (то есть определяется один или несколько блоков данных $\widetilde{\boldsymbol{M}}'_j$ с нарушением целостности, в который входит один или несколько подблоков $\widetilde{\boldsymbol{M}}_{ij}$).

11 Акушский И.Я., Юдицкий Д.М. Машинная арифметика в остаточных классах – М. : Советское радио. 1968. – 604 с.

12 Finko O., Dichenko S. Secure pseudo-random linear binary sequences generators based on arithmetic polynoms // Advances in Intelligent Systems and Computing (см. в книгах). 2015. Vol. 342. Pp. 279–290.

Под нарушением целостности в одном произвольном подблоке данных $\widetilde{M}_{ij}$ кодового слова МПК будем понимать появление однократной ошибки, соответственно q -кратная ошибка определяется как произвольное нарушение целостности q подблоков. Известно, что МПК обнаруживает q ошибок при $k-n \geq q$ и исправляет q или менее ошибок, если $k-n \geq 2q$ [1314] [21].

В соответствии с правилами декодирования модулярных кодов15,16 критерием отсутствия обнаруживаемых ошибок в модулярном коде и МПК (в частности, $\{M_{1j}(z), \dots, M_{nj}(z), \dots, M_{kj}(z)\}_{\text{МПК}}$) является выполнение неравенства: $deg\, X'(z) < deg\, P_n(z)$, где $P_n(z) = \prod_{i=1}^{n} p_i(z)$ и $X'(z)$ – решение системы (5) для $M'_{1j}(z), \dots, M'_{nj}(z), \dots, M'_{kj}(z)$.

Критерий существования обнаруживаемой ошибки – выполнение неравенства $deg\, X'(z) \geq deg\, P_n(z)$ [17].

Восстановление достоверного подблока $M_{ij}(z)$ защищаемых данных выполняется путём вычисления наименьшего вычета: $M_{ij}(z) \equiv X(z)\, mod\, p_{ij}(z)$, где $X(z)$ повторно вычислено с учетом исключения искажённого подблока $\widetilde{M}_{ij}$.

Выполним проверку достоверности восстановленных данных в случае нарушения их целостности путём сравнения значения предварительно вычисленного эталонного хэш-кода $\boldsymbol{H}_i$ (или хэш-кода $\boldsymbol{H}''_i$, вычисленного посредством хэш-функции $h(\boldsymbol{M}'_i)$) со значением вычисленного хэш-кода $\boldsymbol{H}'_i$ уже от восстановленного блока данных.

Оценивание разработанного метода

Оценивание разработанного метода выполняется в сравнении с наиболее популярным из существующих решений комплексного обеспечения целостности данных, в котором последовательно применяются криптографические преобразования к данным – для контроля их целостности и технология резервного копирования – для восстановления целостности данных в случае её нарушения.

При проектировании и разработке новых СХД возникает задача нахождения оптимального решения для контроля и восстановления целостности хранящейся в них информации, то есть обеспечения требуемой устойчивости ИАС через свойство безопасности информации.

Оценивание разработанного метода по показателю качества – вероятность безотказной работы P(t) в течение времени t.

К показателям качества оптимальности защищённых ИАС могут быть отнесены: безопасность (надёжность) хранения, объем вводимой избыточности и прочее.

Разработанный метод при рассмотрении вопросов контроля и восстановления целостности данных является, по сути, инструментом решения задачи обеспечения безопасности (надежности) защищенных ИАС. При этом результативность рассматриваемого решения может быть охарактеризована свойством отказоустойчивости.

Тогда в качестве показателя отказоустойчивости определим вероятность безотказной работы в течение времени $\boldsymbol{t}$ (показатель $\boldsymbol{P(t)}$).

Критерий качества: $\boldsymbol{P(t) \rightarrow max}$.

Вероятность безотказной работы $\boldsymbol{P_1(t)}$ защищенных ИАС, построенных на основе разработанного метода, с функцией восстановления информации по принципу функционирования — скользящее резервирование, соответствует выражению:

$$\boldsymbol{P_1(t) = \sum_{i=0}^{q} \frac{(k-q)\left(\frac{\lambda}{k}t\right)^i}{i!} \cdot exp\left(-(k-q)\frac{\lambda}{k}t\right)}, \quad (7)$$

где k — общее число элементов схемы, q — число резервных элементов схемы, λ — интенсивность отказов.

В свою очередь, вероятность безотказной работы $\boldsymbol{P_2(t)}$ защищенных ИАС, построенных на основе существующего решения (технологии резервного копирования), соответствует выражению:

$$\boldsymbol{P_2(t) = \sum_{i=0}^{d} \frac{(\lambda t)^i}{i!} \cdot exp(-\lambda t)}, \quad (8)$$

где d — кратность резервирования.

Расчёт производится при продолжительности эксплуатации 87600 часов, интенсивность отказов: $\lambda = 0{,}00001\ час^{-1}$. В качестве исходных данных для расчета вероятности безотказной работы рассмотрим избыточные МПК, следующих структур:

— при изменении количества информационных оснований избыточного МПК: $k = \{5,7,11\}$, при $q = 2 - const$;

13 Бояринов И.М. Помехоустойчивое кодирование числовой информации – М. : Наука. 1983. – 386 с.

14 Амербаев В.М. Теоретические основы машинной арифметики – Алма-Ата : Наука. 1976. – 498 с.

15 Торгашов В.А. Система остаточных классов и надежность ЦВМ – М.: Советское радио. 1973. – 329 с.

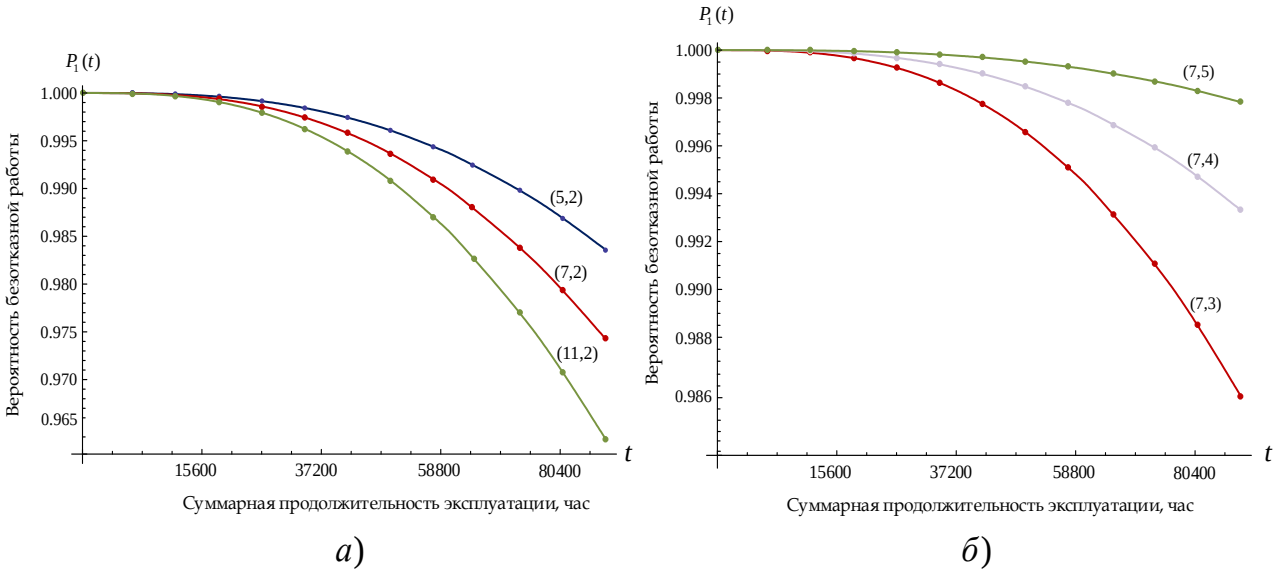
16 Omondi A., Premkumar B. Residue Number Systems: Theory and Implementation. Imperial College Press. London. 2007. – 296 p.

17 Ananda Mohan P.V. Residue Number Systems // Springer International Publishing. 2016. 351 p.

Таблица 1

Расчётные данные вероятности безотказной работы защищённых ИАС, построенных на основе разработанного метода и существующего решения

t, час	$P_1(t)$, при $q = 2$ — const			$P_1(t)$, при $k = 7$ — const			$P_2(t)$
	$k = 5$	$k = 7$	$k = 11$	$q = 3$	$q = 4$	$q = 5$	$d = 2$
8400	0,9999	0,9999	0,9999	0,9999	0,9999	0,999998	0,996664
15600	0,9998	0,9997	0,9996	0,9998	0,9999	0,999986	0,989027
22800	0,9996	0,9993	0,9990	0,9996	0,9998	0,999956	0,977641
30000	0,9991	0,9986	0,9979	0,9992	0,9996	0,999902	0,963064
37200	0,9984	0,9974	0,9962	0,9986	0,9994	0,999815	0,945794
44400	0,9974	0,9958	0,9939	0,9977	0,9990	0,999651	0,926276
51600	0,9960	0,9936	0,9908	0,9965	0,9984	0,999522	0,904906
58800	0,9943	0,9909	0,9870	0,9950	0,9977	0,999303	0,882034
63600	0,9930	0,9888	0,9840	0,9938	0,9972	0,999127	0,866108
73200	0,9898	0,9838	0,9793	0,9910	0,9959	0,998696	0,832999
80400	0,9869	0,9793	0,9769	0,9885	0,9947	0,998298	0,807354
87400	0,9835	0,9942	0,9637	0,9855	0,9933	0,997832	0,781252



а) *б)*

Рис. 6. Зависимость вероятности безотказной работы от структуры применяемого избыточного МПК: а) при $q = 2 - const$, б) при $k = 7 - const$

— при изменении количества контрольных оснований избыточного МПК: $k = 7 - const$, при $q = \{3,4,5\}$.

На основе выражений (7) и (8) получим результаты, приведённые в (табл. 1).

Оценка полученных результатов для расчёта вероятности безотказной работы защищённых ИАС, построенных на основе разработанного метода, представлена на графиках (рис. 6).

Из графического представления полученных результатов видно, что наиболее выигрышным является применение избыточного МПК со структурой: $k = 7$, $q = 5$, а менее выигрышным — при $k = 11$, $q = 2$.

Сравнительная оценка защищённых ИАС, построенных на основе разработанного метода (при $k = 11$, $q = 2$) и существующего решения (при $d = 2$), представлена на графике (рис. 7).

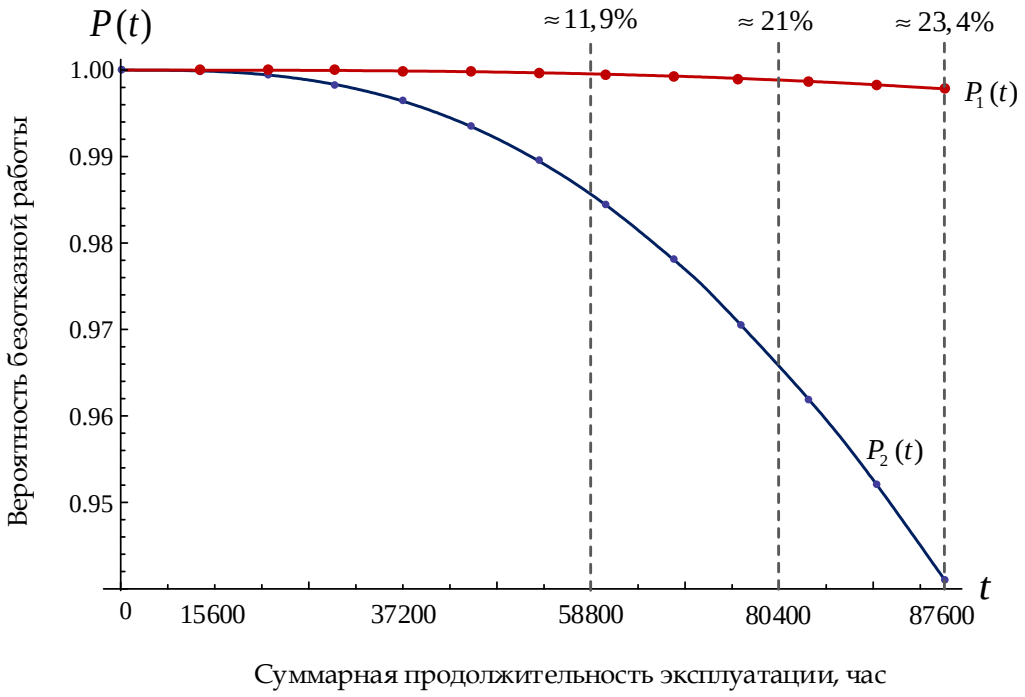


Рис. 7. Зависимость вероятности безотказной работы ИАС, построенных на основе разработанного метода ($P_1(t)$) и существующего решения ($P_2(t)$)

Из графика видно, что вероятность безотказной работы защищенных ИАС, построенной на основе разработанного метода (даже при использовании избыточного МПК с наименее выигрышной структурой: $k = 11$, $q = 2$), выше по отношению к защищенным ИАС, основанным на существующем решении, в частности, на следующих точках:

- при суммарной продолжительности эксплуатации равной 58800 часов выигрыш составляет $\approx 11{,}9\%$;
- при суммарной продолжительности эксплуатации равной 80400 часов выигрыш составляет $\approx 21\%$;
- при суммарной продолжительности эксплуатации равной 87600 часов выигрыш составляет $\approx 23{,}4\%$.

Оценивание разработанного метода по показателю качества – объем вводимой избыточности $V_{изб.}$ при ограничениях на ресурсы СХД

Качество любого объекта в полной мере проявляется лишь в процессе его использования по назначению[18]. Поэтому вопрос обеспечения устойчивости защищённых ИАС является актуальным в первую очередь в условиях деструктивных воздействий злоумышленника и среды при существующих ограничениях на ресурсы СХД.

В этом случае объем вводимой для контроля и восстановления целостности данных избыточности будет иметь большое значение при обеспечении устойчивости защищённых ИАС в процессе их целевого функционирования. Многократное резервирование данных после каждого восстановления их целостности в момент времени t может привести к полному израсходованию ресурсов СХД защищенных ИАС, при котором необходимо будет удалить часть ценной информации, подлежащей хранению в СХД.

Вынужденное удаление части ценной информации, по результатам анализа которой пользователями ИАС принимаются решения, может привести к снижению вероятности выполнения задачи функционирования ИАС или вообще к её невыполнению. Поэтому в качестве показателя качества определим объем вводимой избыточности $V_{изб.}$.

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

Оценивание выполним раздельно для процесса контроля и восстановления целостности данных, хранящихся в СХД.

1. При контроле целостности данных:

- в существующих решениях, где количество вычисляемых хэш-кодов равняется количеству

18 Петухов Г.Б., Якунин В.И. Методологические основы внешнего проектирования целенаправленных процессов и целеустремлённых систем – М. : АСТ. 2006. – 504 с.

блоков данных, подлежащих защите, объем вводимой избыточности будет равен 100%;

— в разработанном методе количество вычисляемых хэш-кодов зависит от размера матрицы (4). Возможные объемы вводимой избыточности представлены в (табл. 2).

Таблица 2

Значения объёма вводимой избыточности $V_{изб.}$

Параметры матрицы (4)	Объем избыточности $V_{изб.}$
$n = 2$	50%
$n = 3$	$\approx 33{,}3\%$
$\vdots$	$\vdots$
$n = 50$	2%

2. При восстановлении целостности данных:

— в существующих решениях, где применяется технология резервного копирования, объем вводимой избыточности при каждом восстановлении целостности равен 100% от общего объёма данных, подлежащих защите;

— в разработанном методе при применении расширенного МПК для восстановления целостности искажённых или утраченных данных потребуется ввод меньшей избыточности. При появлении ошибки в 2-х блоках данных достаточно применить расширенный МПК лишь с 2 избыточными основаниями. В этом случае, избыточность сократится со 100% (при технологии резервного копирования) до $30 - 40\%$ (при использовании разработанного метода).

Таким образом, вероятность выполнения задачи целевого функционирования защищённой ИАС зависит от количества выполненных задач пользователями ИАС по принятию решений, правильность которых зависит от достоверности и полноты анализируемых данных, хранящихся в СХД. Схема, поясняющая зависимость вероятности выполнения задачи целевого функционирования от ресурса СХД, представлена на (рис. 8).

Использование для обеспечения устойчивости ИАС существующих решений, характеризуемых вводом высокой избыточности, приводит в условиях деструктивных воздействий к израсходованию ресурсов СХД (y_2) за счет многократного повторения процедуры резервного копирования и вычисления эталонных хэш-кодов. При этом происходит снижение количества выполненных задач пользователями ИАС по принятию правильных решений (z_2) и, как следствие – снижение вероятности выполнения задачи целевого функционирования ИАС (x_2).

В то же время, при использовании разработанного метода вероятность выполнения задачи целевого функционирования ИАС (x_1) увеличивается за счет увеличения количества выполненных задач пользователями

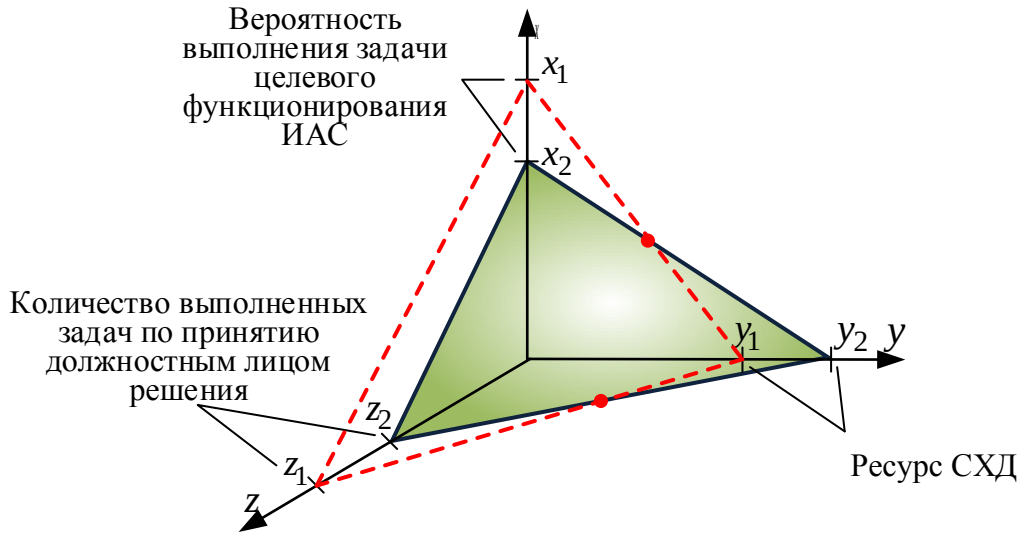


Рис. 8. Зависимость вероятности выполнения задачи целевого функционирования защищённых ИАС от израсходования ресурса применяемых СХД

ИАС по принятию правильных решений (z_1), напрямую связанных с ресурсом применяемых СХД (y_1).

Выводы

В работе представлен один из способов формализованного представления данных в многомерных СХД, позволяющий построить математическую модель процесса контроля и восстановления целостности данных в защищённых ИАС на основе крипто-кодовых преобразований. Представленная модель, основанная на агрегировании криптографических методов и методов помехоустойчивого кодирования, позволяет за счет объединения свойств функции хэширования (контроль целостности данных с криптографической стойкостью) и помехоустойчивого кода (обнаружение и исправление ошибок с заданной вероятностью), получить новое свойство – обеспечение подтверждённой целостности данных в условиях деструктивных воздействий злоумышленника и среды.

За счёт появляющейся эмерджентности на примере разработанного метода показана возможность расширения функционала защищённых ИАС, связанная с подтверждением достоверности восстановления целостности искажённых или утраченных данных.

В целом предложенный метод, учитывающий структуру многомерного представления в СХД данных, позволяет обеспечить устойчивость защищённых ИАС в условиях деструктивных воздействий за счёт осуществления контроля и восстановления целостности данных на уровне аппаратурных и программных затрат, соответствующих наиболее эффективным методам обеспечения надёжности и безопасности.

Получены расчётные данные вероятности безотказной работы защищённых ИАС, построенных на основе разработанного метода, с функцией восстановления информации по принципу функционирования – скользящее резервирование. Показана зависимость вероятности выполнения задачи целевого функционирования защищённых ИАС от объема вводимой для контроля и восстановления целостности данных избыточности.

Литература

1. Reinsel D., Gantz J., Rydning J. Data Age 2025: The Evolution of Data to Life-Critical // International Data Corporation. 2017. – Pp. 1–27.
2. Dedić N., Stanier C. Towards Differentiating Business Intelligence, Big Data, Data Analytics and Knowledge Discovery // Springer International Publishing. 2017. – Pp. 114 – 122.
3. Onay C., Öztürk E. A review of credit scoring research in the age of Big Data // Journal of Financial Regulation and Compliance. 2018. № 26(3).– Pp. 382–405.
4. Диченко С.А. Модель угроз безопасности информации защищённых информационно-аналитических систем специального назначения // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2022. № 1–2 (163–164). – С. 64–71.
5. Калюжный А.В., Максимов В.А., Шушаков А.О. Модель функционирования гетерогенной бортовой системы хранения данных с учетом неоднородной информационной важности хранимых данных // Труды Военно-космической академии имени А.Ф. Можайского. 2019. №671. С. 33 – 40.
6. Хомоненко А.Д., Басыров А.Г., Бубнов В.П., Забродин А.В., Краснов С.А., Лохвицкий В.А., Тырва А.В. Модели и методы исследования информационных систем. – СПб. : Лань. 2019. – 204 с.
7. Павлов А.Н., Слинько А.А., Воротягин В.Н. Методика оценивания структурно-функциональной живучести бортовых систем малых космических аппаратов в условиях возникновения нерасчетных полетных ситуаций // Информация и космос. 2019. № 2. С. 139–147.
8. Бучинский Д.И., Вознюк В.В., Фомин А.В. Исследование помехоустойчивости приёмника сигналов с многопозиционной фазовой манипуляцией к воздействию помех с различной структурой // Труды Военно-космической академии имени А.Ф. Можайского. 2019. № 671. С. 120 – 127.
9. Носов А.П., Ахрем А.А., Рахманкулов В.З. Анализ эффективности декомпозиции OLAP-гиперкубов данных для методов экспоненциальной вычислительной сложности // Математика и математическое моделирование. 2021. № 3. С. 29–45.
10. Бопп В.А. Технология резервного копирования. преимущества и недостатки // Известия Тульского государственного университета. Технические науки. 2019. № 3. С. 134–137.
11. Диченко С.А. Модель контроля целостности многомерных массивов данных // Проблемы информационной безопасности. Компьютерные системы. 2021. № 2 (46). – С. 97–103.
12. Сапожников В.В. Основы теории надежности и технической диагностики // СПб.: Лань. 2019. – 588 с.
13. Финько О.А., Диченко С.А. Гибридный крипто-кодовый метод контроля и восстановления целостности данных для защищённых информационно-аналитических систем // Вопросы кибербезопасности. 2019. №6(34). С. 17–36. DOI:10.21681/2311-3456-2019-6-17-36
14. Dichenko S.A., Finko O.A. Controlling and restoring the integrity of multi-dimensional data arrays through cryptocode constructs // Programming and Computer Software. 2021. Vol. 47. No. 6. – Pp. 415–425.
15. Dichenko S., Finko O. Two-dimensional control and assurance of data integrity in information systems based on residue number system codes and cryptographic hash functions // В сборнике: Integrating Research Agendas and Devising Joint Challenges. International Multidisciplinary Symposium ICT Research in Russian Federation and Europe. 2018. Pp. 139–146.

16. Dichenko S.A. An integrity control model for multidimensional data arrays // Automatic Control and Computer Sciences. 2021. Vol. 55. No. 8. Pp. 1188–1193.
17. Samoylenko D., Eremeev M., Finko O., Dichenko S. Protection of information from imitation on the basis of crypt-code structures // Advances in Intelligent Systems and Computing (см. в книгах). 2019. Vol. 889. Pp. 317–331.
18. Kalmykov I., Chistousov N., Aleksandrov A., Provornov I. Application of correcting polynomial modular codes in infotelecommunication systems // Advances in Intelligent Systems and Computing. 2020. Т. 1226. С. 387–398.
19. Балюк А.А., Финько О.А. Многоагентная аутентификация цифровых двойников в киберфизических системах // Вопросы кибербезопасности. 2022. № 5 (51). С. 100 –113.
20. Шарапов И.О., Самойленко Д.В., Кушпелев А.С. Математическая модель имитозащищенной обработки данных в робототехнических комплексах на основе криптокодовых конструкций // Автоматизация процессов управления. 2022. № 1 (67). С. 106–114.
21. Samoylenko D.V., Eremeev M.A., Finko O.A., Dichenko S.A. Parallel linear generator of multivalued pseudorandom sequences with operation errors control // SPIIRAS Proceedings. 2018. No. 4 (59). Pp. 31–61.

A METHOD OF PARAMETRIC SYNTHESIS OF CRYPTO-CODE STRUCTURES FOR MONITORING AND RESTORING THE INTEGRITY OF INFORMATION

Dichenko S.A.[19], Samoylenko D.V.[20], Finko O.A.21, Ryumshin K.Yu.[22]

The purpose of the work *is to develop a method for monitoring and restoring the integrity of information in secure multidimensional data storage systems that ensures the stability of the systems under consideration under the destructive influences of an intruder and disturbances in the operating environment.*

Research method: *in the course of the research, the scientific and methodological apparatus of the theory of algebraic systems was used in conjunction with the methods of cryptographic information protection and the mathematical apparatus of coding theory to implement the procedures of crypto-code transformations. Models of reliable data storage systems were studied to justify the feasibility of procedures for ensuring the confirmed integrity of the processed information.*

Results of the study: *a method for formalized representation of information in secure multidimensional data storage systems used in the interests of information and analytical systems, which makes it possible to visually describe the developed structures for monitoring and restoring data integrity under the destructive influences of an intruder and disturbances in the operating environment. A mathematical model of the process of monitoring and restoring data integrity based on crypto-code transformations based on the aggregation of cryptographic methods and methods of error-correcting coding is presented. Combining well-known classical solutions to ensure data integrity will reduce the introduced redundancy, as well as expand the functionality of secure information and analytical systems, which consists in confirming the reliability of restoring the integrity of distorted or lost data without additional costs of their repeated control by cryptographic methods. The proposed model takes into account the structure of multidimensional representation of information in the considered data storage systems of information and analytical systems.*

Scientific novelty: *the developed method of parametric synthesis of crypto-code structures for monitoring and restoring the integrity of information in secure multidimensional data storage systems differs from the known ones by obtaining optimal crypto-code structures due to the rational aggregation of cryptographic and code transformations in the parameter space of the considered data storage systems. Crypto-code structures formed*

19 Sergey A. Dichenko, Ph. D, Krasnodar Higher Military School them. Army General S.M. Shtemenko, Krasnodar, Russia. E-mail: dichenko.sa@yandex.ru

20 Dmitry V. Samoilenko, Dr.Sc., Associate Professor, Krasnodar Higher Military School. Army General S.M. Shtemenko, Krasnodar, Russia. E-mail: sam-0019@yandex.ru

21 Oleg A. Finko, Dr.Sc., Professor, Krasnodar Higher Military School named after I.I. Army General S.M. Shtemenko, Krasnodar, Russia. E-mail: ofinko@yandex.ru

22 Konstantin Yu. Ryumshin, Dr.Sc., Moscow Technical University of Communications and Informatics, Moscow, Russia. E-mail: e8@mail.ru

on the basis of building multidimensional hash codes and performing transformations in extended Galois fields provide cryptographic control and restoration of information integrity with the possibility of flexible introduction of redundancy and confirmation with cryptographic reliability of information integrity after the restoration procedure.

Keywords: *information-analytical systems, Big Data, multidimensional data representation, verified integrity, cryptographic methods, hash function, error-correcting coding, crypto-code constructions, emergence.*

References

1. Reinsel D., Gantz J., Rydning J. Data Age 2025: The Evolution of Data to Life-Critical // International Data Corporation. 2017. – Pp. 1–27.
2. Dedić N., Stanier C. Towards Differentiating Business Intelligence, Big Data, Data Analytics and Knowledge Discovery // Springer International Publishing. 2017. – Pp. 114 – 122.
3. Onay C., Öztürk E. A review of credit scoring research in the age of Big Data // Journal of Financial Regulation and Compliance. 2018. № 26(3).– Pp. 382–405.
4. Dichenko S.A. Model' ugroz bezopasnosti informacii zashhishhjonnyh informacionno-analiticheskih sistem special'nogo naznachenija // Voprosy oboronnoj tehniki. Serija 16: Tehnicheskie sredstva protivodejstvija terrorizmu. 2022. № 1–2 (163–164). – S. 64–71.
5. Kaljuzhnyj A.V., Maksimov V.A., Shushakov A.O. Model' funkcionirovanija geterogennoj bortovoj sistemy hranenija dannyh s uchetom neodnorodnoj informacionnoj vazhnosti hranimyh dannyh // Trudy Voenno-kosmicheskoj akademii imeni A.F. Mozhajskogo. 2019. №671. S. 33 – 40.
6. Homonenko A.D., Basyrov A.G., Bubnov V.P., Zabrodin A.V., Krasnov S.A., Lohvickij V.A., Tyrva A.V. Modeli i metody issledovanija informacionnyh sistem. – SPb. : Lan'. 2019. – 204 s.
7. Pavlov A.N., Slin'ko A.A., Vorotjagin V.N. Metodika ocenivanija strukturno-funkcional'noj zhivuchesti bortovyh sistem malyh kosmicheskih apparatov v uslovijah vozniknovenija neraschetnyh poletnyh situacij // Informacija i kosmos. 2019. № 2. S. 139–147.
8. Buchinskij D.I., Voznjuk V.V., Fomin A.V. Issledovanie pomehoustojchivosti prijomnika signalov s mnogopozicionnoj fazovoj manipuljaciej k vozdejstviju pomeh s razlichnoj strukturoj // Trudy Voenno-kosmicheskoj akademii imeni A.F. Mozhajskogo. 2019. № 671. S. 120 – 127.
9. Nosov A.P., Ahrem A.A., Rahmankulov V.Z. Analiz jeffektivnosti dekompozicii OLAP-giperkubov dannyh dlja metodov jeksponencial'noj vychislitel'noj slozhnosti // Matematika i matematicheskoe modelirovanie. 2021. № 3. S. 29–45.
10. Bopp V.A. Tehnologija rezervnogo kopirovanija. preimushhestva i nedostatki // Izvestija Tul'skogo gosudarstvennogo universiteta. Tehnicheskie nauki. 2019. № 3. S. 134–137.
11. Dichenko S.A. Model' kontrolja celostnosti mnogomernyh massivov dannyh // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2021. № 2 (46). – S. 97–103.
12. Sapozhnikov V.V. Osnovy teorii nadezhnosti i tehnicheskoj diagnostiki // SPb.: Lan'. 2019. – 588 s.
13. Fin'ko O.A., Dichenko S.A. Gibridnyj kripto-kodovyj metod kontrolja i vosstanovlenija celostnosti dannyh dlja zashhishhjonnyh informacionno-analiticheskih sistem // Voprosy kiberbezopasnosti. 2019. №6(34). S. 17–36. DOI:10.21681/2311-3456-2019-6-17-36
14. Dichenko S.A., Finko O.A. Controlling and restoring the integrity of multi-dimensional data arrays through cryptocode constructs // Programming and Computer Software. 2021. Vol. 47. No. 6. – Pp. 415–425.
15. Dichenko S., Finko O. Two-dimensional control and assurance of data integrity in information systems based on residue number system codes and cryptographic hash functions // V sbornike: Integrating Research Agendas and Devising Joint Challenges. International Multidisciplinary Symposium ICT Research in Russian Federation and Europe. 2018. Pp. 139–146.
16. Dichenko S.A. An integrity control model for multidimensional data arrays // Automatic Control and Computer Sciences. 2021. Vol. 55. No. 8. Pp. 1188–1193.
17. Samoylenko D., Eremeev M., Finko O., Dichenko S. Protection of information from imitation on the basis of crypt-code structures // Advances in Intelligent Systems and Computing (sm. v knigah). 2019. Vol. 889. Pp. 317–331.
18. Kalmykov I., Chistousov N., Aleksandrov A., Provornov I. Application of correcting polynomial modular codes in infotelecommunication systems // Advances in Intelligent Systems and Computing. 2020. T. 1226. S. 387–398.
19. Baljuk A.A., Fin'ko O.A. Mnogoagentnaja autentifikacija cifrovyh dvojnikov v kiberfizicheskih sistemah // Voprosy kiberbezopasnosti. 2022. №5 (51). S. 100 –113.
20. Sharapov I.O., Samojlenko D.V., Kushpelev A.S. Matematicheskaja model' imitozashhishhennoj obrabotki dannyh v robototehnicheskih kompleksah na osnove kriptokodovyh konstrukcij // Avtomatizacija processov upravlenija. 2022. № 1 (67). S. 106–114.
21. Samoylenko D.V., Eremeev M.A., Finko O.A., Dichenko S.A. Parallel linear generator of multivalued pseudorandom sequences with operation errors control // SPIIRAS Proceedings. 2018. No. 4 (59). Pp. 31–61.