УДК 004.822

ОНТОЛОГИЯ КОНЕЧНО-АВТОМАТНОЙ КРИПТОГРАФИИ

А.А. Шарипбай[1], Ж.С. Сауханова[2], Г.Б. Шахметова[3], М.С. Сауханова[4]

Евразийский национальный университет им. Л.Н. Гумилева, Астана, Казахстан
[1] sharalt@mail.ru, [2] saukhanova@mail.ru, [3] shakhmetova.gb@gmail.com, [4] m.saukhanova@mail.ru

Аннотация

На сегодняшний день совершенствование методов защиты информации является актуальной задачей. Статья посвящена применению альтернативных методов разработки более стойких и эффективных криптосистем с открытыми ключами. В качестве модели приняты конечные автоматы. Для систематизации знаний в области конечно-автоматной криптографии использована онтология. В работе рассматриваются вопросы построения онтологической модели конечно-автоматной криптографии. Предлагаемая онтологическая модель имеет четыре основных уровня: онтология представления знаний, онтология верхнего уровня, онтология предметной области и прикладные онтологии. В качестве онтологии представления знаний использована методология концептуальных карт. Онтология верхнего уровня содержит основную информацию о криптографии и теории автоматов, онтология предметной области описывает непосредственно конечно-автоматную криптографию. В качестве примера прикладной онтологии был рассмотрен алгоритм криптосистемы с открытым ключом на основе конечных автоматов. Представленная онтология построена впервые и даёт чёткое понимание применения конечных автоматов в криптографии, систематизирует полученные в ходе исследования сведения о данной предметной области, является предпосылкой дальнейшей разработки криптосистем, основанных на теории автоматов.

Ключевые слова: *онтология, концептуальная карта, конечный автомат, криптография.*

Цитирование: *Шарипбай, А.А.* Онтология конечно-автоматной криптографии / А.А. Шарипбай, Ж.С. Сауханова, Г.Б. Шахметова, М.С. Сауханова // Онтология проектирования. – 2019. – Т.9, №1(31). – С.36-49. – DOI: 10.18287/2223-9537-2019-9-1-36-49.

Введение

В условиях быстрого развития информационных технологий и внедрения их во все сферы человеческой деятельности обеспечение надёжной защиты информации, передаваемой по незащищённым каналам связи, становится актуальной проблемой современного общества. Известно, что криптография занимается исследованием методов преобразования (шифрования и дешифрования) информации с целью скрытия её содержания [1, 2], а одним из перспективных направлений в криптографии является применение теории конечных автоматов (КА) для шифрования и дешифрования информации.

Для систематизации знаний в области конечно-автоматной криптографии (КАКГ) было принято решение использовать *онтологию*. Известно, что онтология позволяет концептуализировать предметную область (ПрО), формализовать накопленные знания: определить ключевые понятия, задать семантические отношения между понятиями, необходимые для постановки задач и описания процессов их решения в данной ПрО. Кроме того, преимуществом использования онтологии является возможность анализа, накопления и повторного применения знаний о ПрО, полученной из разных источников [3]. Поэтому основной целью настоящей статьи является построение онтологической модели КАКГ.

В качестве инструмента был выбран общедоступный и хорошо себя зарекомендовавший на практике программный продукт CmapTools [4], который используется для построения концептуальных карт (К-карт).

1 Особенности создания онтологий с помощью концептуальных карт

При исследовании ПрО необходима систематизация полученных знаний. Область исследования можно представить в виде *концептуальной модели* ПрО, которая содержит в себе множества понятий (концептов), классификацию, свойства и характеристики этих понятий. В настоящее время применяют *онтологию* для наглядного представления концептуальной модели ПрО. Под онтологией понимается «формальная спецификация концептуализации, которая имеет место в некотором контексте ПрО» [5].

Формально онтологию можно определить следующим образом [6]:

O = <C, R, A>, где:

- C – конечное множество концептов (понятий, терминов) ПрО;
- R – конечное множество отношений между концептами (понятиями, терминами) ПрО;
- A – конечное множество аксиом или функций интерпретации, заданных на концептах и (или) отношениях.

Для построения онтологической модели КАКГ выбрана методология концептуальных карт (concept maps, К-карт). К-карта позволяет графически представить знания изучаемой ПрО. Она представляет собой ациклический граф, вершины которого есть основные понятия (концепты) рассматриваемой ПрО, а ребра – связи между понятиями (отношения) [7]. «Концепты и связи между ними имеют универсальный характер для некоторого класса понятий ПрО. Поэтому любая разработка К-карты подразумевает анализ структурных взаимодействий между отдельными понятиями ПрО» [8]. На рисунке 1 показан пример построения онтологии К-карты с помощью инструмента CmapTools.

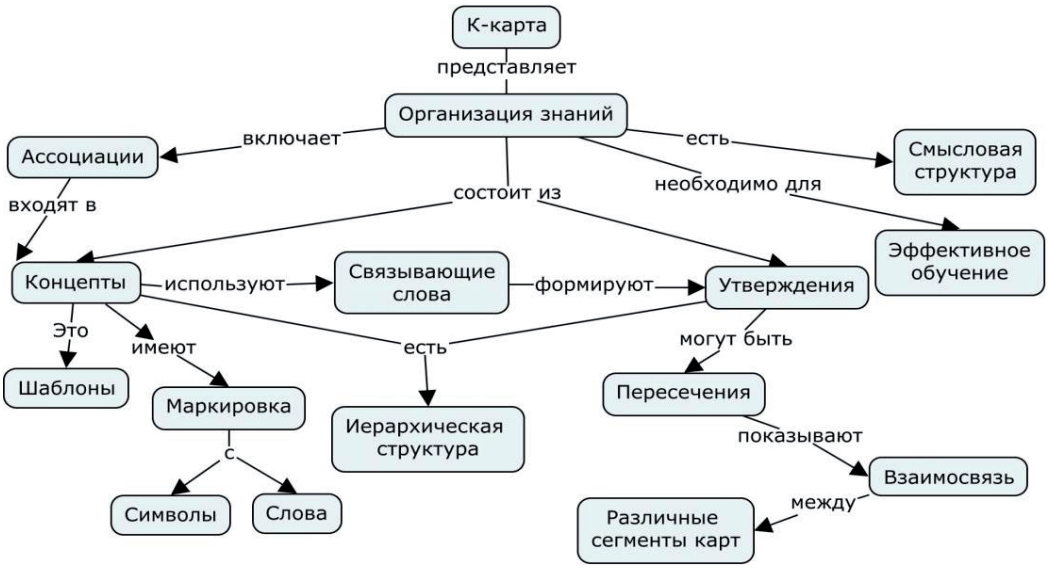

Рисунок 1 – Онтология К-карты

К-карты можно отнести к «лёгким» онтологиям, которые не содержит аксиом [9] и имеют вид:

O_k = (C, R), где: C – конечное множество концептов ПрО; R – множество отношений между концептами.

Выбор К-карт для создания онтологической модели КАКГ обусловлен их следующими преимуществами [6]:

- *системность* – К-карты позволяют представить целостный взгляд на изучаемую ПрО;
- *единообразие* – материал воспроизводится и воспринимается эффективней, если представлен в единой форме;

- *научность* – формирование К-карты ПрО позволяет выявить недостающие логические связи во всей их полноте;
- *когнитивность* – в процессе построения К-карт используются все виды памяти человека, что позволяет быстро запоминать представленные картами сведения об изучаемой ПрО.

Рассматриваемая ПрО представляет собой сложно-структурированную область и включает в себя понятия криптографии, теории автоматов и прикладную терминологию, содержащую понятия по конкретным реализациям криптосистем, основанных на КА. Онтологию КАКГ можно разделить на четыре основных уровня, которые показаны на рисунке 2.

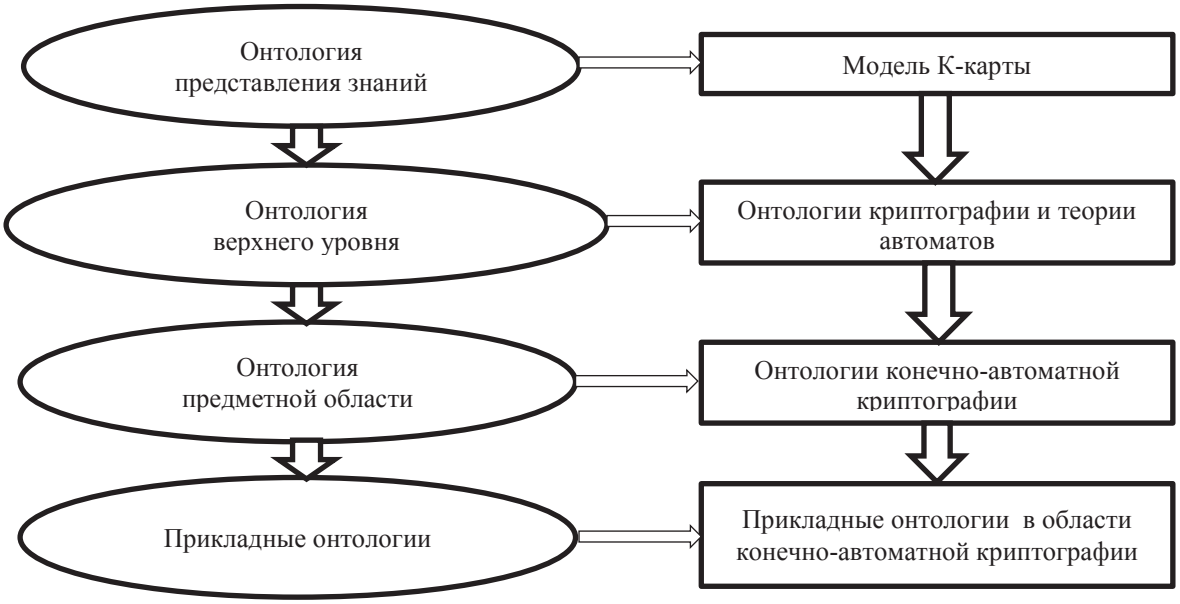

Рисунок 2 – Уровни онтологической модели области конечно-автоматной криптографии

Первый уровень – онтология представления знаний – описывает область представления знаний. Целью первого уровня является создание языка для спецификаций других онтологий более низкого уровня. В качестве онтологии первого уровня использована модель К-карты, показанной на рисунке 1.

Онтология верхнего уровня – это онтология криптографии и теории автоматов, поскольку ПрО объединяет криптографию и теорию КА.

Третий уровень онтологии – это онтология КАКГ, в которой даются описания основных концептов конечно-автоматной модели. По своей структуре онтология КАКГ является логическим продолжением онтологии верхнего уровня.

Четвёртый уровень онтологии – это прикладные технологии КАКГ. Данный уровень содержит специфичную информацию – концепты и отношения, которые раскрывают особенности определённых криптосистем, основанных на КА.

2 Онтология конечно-автоматной криптографии

КАКГ основана на использовании теории автоматов и криптографии. Каждая из этих наук включает в себя огромный понятийный аппарат. В статье выбраны основные концепты, которые дают ясное представление об изучаемой ПрО. На рисунке 3 показано объединение данных направлений. В верхней части рисунка 3 (а) концептуальной модели расположены основные концепты и отношения, относящиеся к криптографии, нижняя часть рисунка 3 (с)

содержит важные концепты и связи теории автоматов, на стыке двух онтологий (рисунок 3 (b)) представлены существующие криптосистемы, построенные на основе КА.

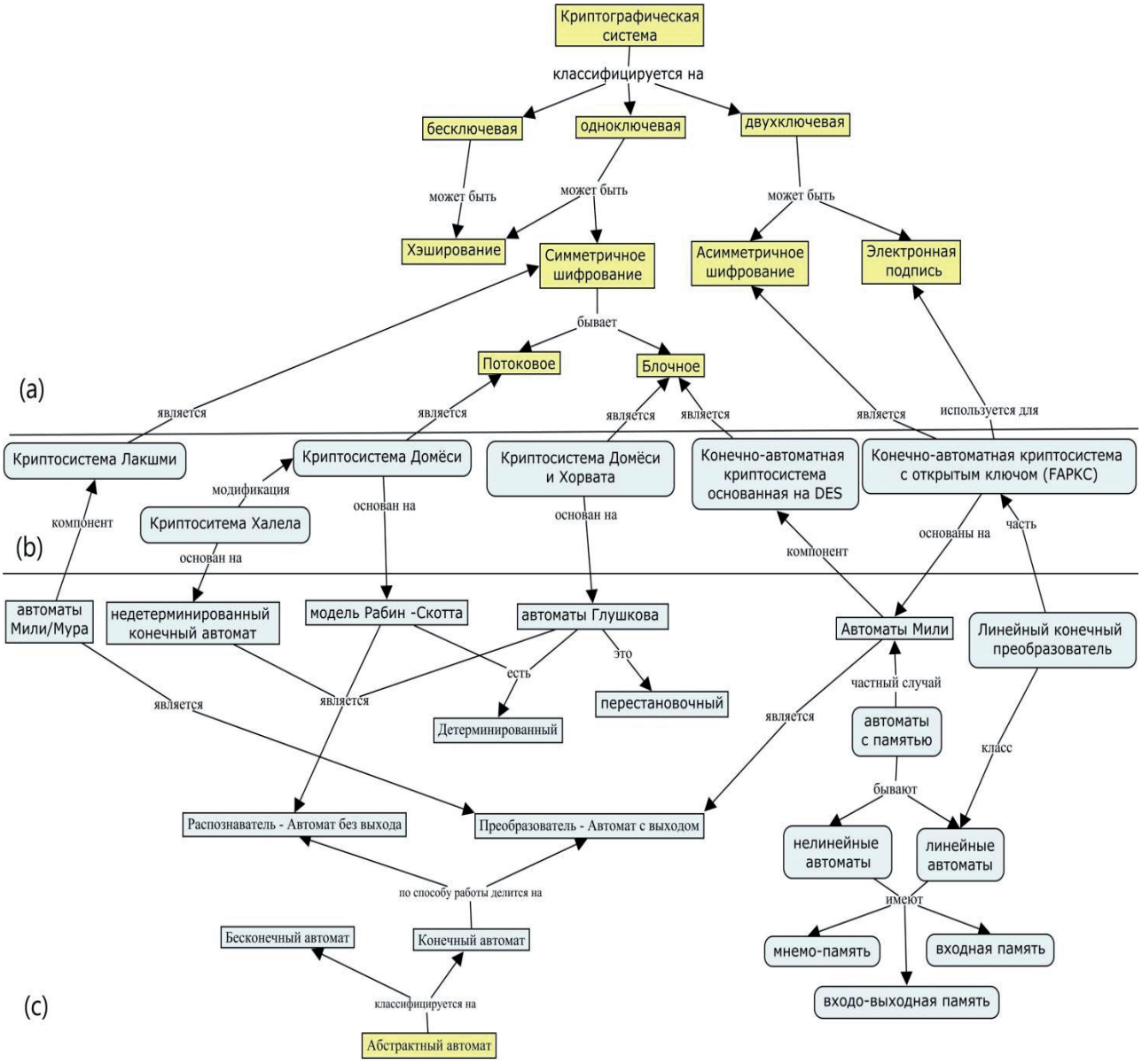

Рисунок 3 – Онтология конечно-автоматной криптографии

В онтологической модели криптографии вершиной является криптографическая система. Криптографическая система представляет собой набор из криптографического алгоритма, открытого и закрытого текстов и ключей. Криптографический алгоритм (шифр) – это математическая функция, которая используется для преобразования открытого текста в зашифрованный (шифрование) и обратно (дешифрование) [10]. Ключ является основным компонентом шифра, который непосредственно отвечает за выбор преобразований криптотекста и хранится в тайном месте. В зависимости от числа ключей криптографические системы разделяют на бесключевые, одноключевые и двухключевые.

Бесключевая криптографическая система реализует метод хэширования (*hashing*) или контрольное преобразование информации. Одноключевая криптосистема – это способ симметричного шифрования, в котором используется один секретный ключ, как для шифрова-

ния, так и для дешифрования. Симметричная криптосистема подразделяется на блочное и потоковое шифрование. Двухключевая криптосистема применяется в асимметричном шифровании и в электронной цифровой подписи. В асимметричном шифровании используют два типа ключей: открытые – для шифрования исходного текста, и секретные – для дешифрования зашифрованного текста. Оба эти ключа связаны между собой сложным соотношением. Электронная цифровая подпись необходима для подтверждения целостности и авторства данных [11].

Криптографические системы, основанные на КА – это алгоритмы, в качестве ключей которых используются КА. В вершине онтологии теории автоматов лежит концепт «Абстрактный автомат» (АА). Согласно [12] АА – это модель дискретного устройства, которое описано пятиместным кортежем:

$A = <X, Y, S, \delta, \lambda>$, где:

X – множество входных символов;

Y – множество выходных символов;

S – множество внутренних состояний;

$\delta: S \times X \rightarrow S$– функция переходов;

$\lambda: S \times X \rightarrow Y$– функция выходов.

В случае, когда множества X, Y, S – конечны, АА является КА. Если хотя бы одно из перечисленных множеств бесконечно, то АА называется *бесконечным*.

По принципу однозначности функции перехода КА можно классифицировать как *детерминированный* или *недетерминированный КА*.

Детерминированность автомата заключается в выполнении условия однозначности переходов, т.е., если автомат находится в некотором состоянии и под воздействием произвольного входного символа переходит в одно и только одно состояние. При недетерминированности КА, он под воздействием одного и того же входного символа может перейти в различные состояния из множества состояний S [13].

По способу работы КА разделяют на два вида [14]:

- *автомат – преобразователь (автомат с выходом):* данный вид автомата преобразовывает поступившую на входе информацию в выходную последовательность, т.е. реализует автоматные отображения;
- *автомат – распознаватель (автомат без выхода):* данный вид автомата распознаёт поступившую на вход последовательность, т.е. отвечает на вопрос: принадлежит ли входная последовательность к данному множеству.

В класс преобразователей входят автоматы Мили/Мура. Согласно [15] данные автоматы имеют следующую формальную запись:

Автомат Мили: $\begin{cases} s(t+1) = \delta\big(s(t), x(t)\big) \\ y(t) = \lambda(s(t), x(t)) \end{cases}$, t=0,1,2,…

Автомат Мура: $\begin{cases} s(t+1) = \delta\big(s(t), x(t)\big) \\ y(t) = \lambda(s(t)) \end{cases}$, t=0,1,2,…

КА Мили, находясь в начальном состоянии $s(0)$, под действием входной последовательности $x(0)x(1)$... проходит последовательность состояний $s(0)s(1)$... и вырабатывает выходную последовательность $y(0)y(1)$… . Зависимость между входными символами, состояниями автомата и выходными символами в дискретном времени t показана с помощью данных систем канонических уравнений.

В автоматах Мура, в отличие от автоматов Мили, выходная последовательность определяется только состоянием автомата в какой-то момент времени t и не зависит от входной последовательности в этот же момент времени.

Как видно из рисунка 3 автомат с памятью является частным случаем автомата Мили. Данные автоматы применяются в реализации конечно-автоматной криптосистемы с открытым ключом (FAPKC). Согласно [16], если функция $\varphi: Y^k \times X^{h+1} \to Y$ для некоторых целых $k,\ h \geq 0$, и если КА $M = < X, Y, Y^k \times X^{h+1}, \delta, \lambda >$ может быть определён $y(i) = \varphi\big(y(i-1), \dots, y(i-k), x(i), \dots, x(i-h)\big)$, *i = 0, 1, . . .*, а именно

$$\delta(< y_{-1}, \dots, y_{-k}, x_{-1}, \dots, x_{-h} >, x_0) = < y_0, \dots, y_{-k+1}, x_0, \dots, x_{-h+1} >,$$

$$\lambda(< y_{-1}, \dots, y_{-k}, x_{-1}, \dots, x_{-h} >, x_0) = < y_0, \dots, y_{-k+1}, x_0, \dots, x_{-h+1} >,$$

$$y_0 = \varphi(y_{-1}, \dots, y_{-k}, x_0, \dots, x_{-h}),$$

тогда *M* называется КА с *памятью порядка (h, k)* и обозначается через M_φ. Тогда *h* и *k* называются *входной* и *выходной* памятью автомата *M* соответственно. В случае, когда *k=0, автомат* M_φ называется КА с *входной памятью порядка h.*

Пусть функция $f: Y^k \times U^{p+1} \times X^{h+1} \to Y$, а функция $g: Y^k \times U^{p+1} \times X^{h+1} \to U$ для некоторых целых *k,* $h \geq 0$, $p \geq -1$, и если КА $M_{f,g} = < X, Y, Y^k \times U^{p+1} \times X^h, \delta, \lambda >$ может быть определён $y(i) = f\big(y(i-1), \dots, y(i-k), u(i), \dots, u(i-p), x(i), \dots, x(i-h)\big)$,

$u(i+1) = g\big(y(i-1), \dots, y(i-k), u(i), \dots, u(i-p), x(i), \dots, x(i-h)\big)$, *i* = 0,1, …

а именно

$\delta\big(< y_{-1}, \dots, y_{-k}, u_0, \dots, u_{-p}, x_{-1}, \dots, x_{-h} >, x_0\big) = < y_0, \dots, y_{-k+1}, u_1, \dots, u_{-p+1}, x_0, \dots, x_{-h+1} >,$

$\lambda\big(< y_{-1}, \dots, y_{-k}, u_0, \dots, u_{-p}, x_{-1}, \dots, x_{-h} >, x_0\big) = < y_0, \dots, y_{-k+1}, u_1, \dots, u_{-p+1}, x_0, \dots, x_{-h+1} >,$

$y_0 = f(y_{-1}, \dots, y_{-k}, u_0, \dots, u_{-p}, x_0, \dots, x_{-h}),$

$u_1 = g(y_{-1}, \dots, y_{-k}, u_0, \dots, u_{-p}, x_0, \dots, x_{-h}),$

тогда *M* называется КА *с псевдо-памятью порядка (h,k,p)* и обозначается через $M_{f,g}$.

Автомат с памятью подразделяют на *линейные* и *нелинейные*. Если функции, определяющие КА, линейны, то автомат является линейным (ЛКА). Добавление к ЛКА любой нелинейной функции приводит к *нелинейному КА* с памятью (НлКА).

Рассмотрим КА в качестве распознавателя.

Если для КА *A* = <*X,Y,S,δ,λ*>, |*Y*| = 1, то он называется автоматом без выхода и определяется тройкой <*X, S, δ*>.

Если <*X, S, δ*> КА без выхода, $s_0 \in S$ – начальное состояние, $F \subseteq S$ – конечное множество финальных состояний, тогда пятерка $< X, S, \delta, s_0, F >$ называется КА – *распознаватель*.

КА $A = < X, S, \delta >$ с *S* = *X* называется *перестановочным автоматом*, если для любых *a, b* $\in S$ ($a \neq b$) и *x, y* $\in X$ ($x \neq y$), $\delta(a, x) \neq \delta(b, x)$ *и* $\delta(a, x) \neq \delta(a, y)$.

Модель Рабин-Скотта – это детерминированный КА - распознаватель.

3 Онтология ПрО

Модель включает в себя концепты из описанных в разделах 1 и 2 уровней и новые понятия, относящиеся непосредственно к КАКГ (см. рисунок 4). В КАКГ введены следующие концепты: композиция КА, обратимость КА, слабо обратимый КА с задержкой, обратный автомат. Эти характеристики стали основополагающими в разработке криптосистем на основе КА. Как показано на рисунке 3, криптосистема FAPKC основана на КА Мили, а именно на КА с памятью. Основная идея FAPKC заключается в использовании последовательной композиции слабо обратимых КА для генерации открытого ключа, тогда как секретный ключ состоит из их обратных КА. Данная семантическая связь видна на рисунке 4. Дадим определение концептов.

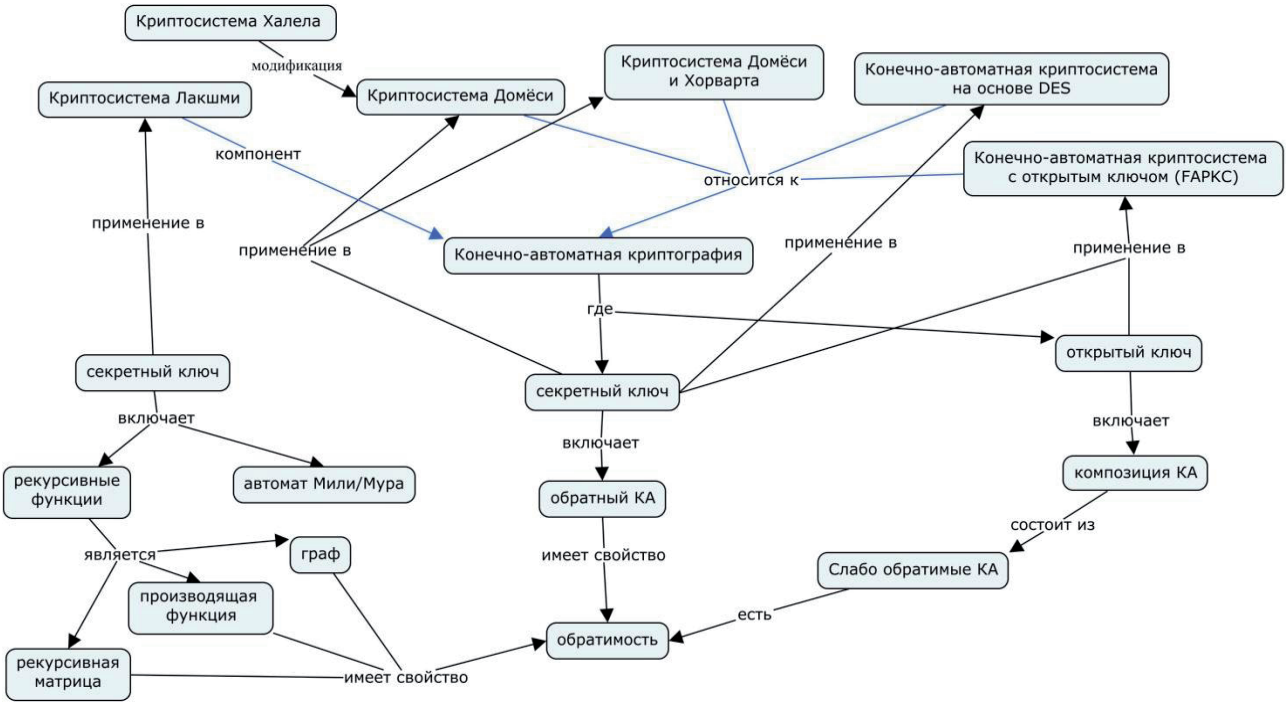

Рисунок 4 – Онтология предметной области

Пусть даны два КА $M =< X, Y, S, \delta, \lambda >$ и $M' =< X, Y, S', \delta', \lambda' >$. КА $M =< X, Y, S, \delta, \lambda >$ называется *слабо обратимым с задержкой* τ, где τ – целое неотрицательное число, если $\forall s \in S$ и $\forall x_i \in X, i = 0,1, \dots \tau$, x_0 может быть однозначно определено состоянием s и функцией выхода $\lambda(s, x_0 \dots x_\tau)$.

Для $\forall s \in S$ и $\forall s' \in S'$, если $\forall a \in X^\omega, \exists a_0 \in X^k: \lambda'(s', \lambda(s, a)) = a_0 a$ и $|\alpha_0| = \tau$, тогда (s', s) называется парой с задержкой τ (τ-*парой*), т.е. s' соответствует s с задержкой τ [17].

Автомат M' называется *обратным с задержкой* τ к автомату M, если $\forall s \in S\ \exists s' \in S'$ такой что *(s', s)* является τ-парой в $M' \times M$.

Пусть заданы два КА $M_1 =< X_1, Y_1, S_1, \delta_1, \lambda_1 >$ и $M_2 =< X_2, Y_2, S_2, \delta_2, \lambda_2 >$, где $X_2 = Y_1$. Тогда композиция двух КА, определяется так:

$$C(M_1, M_2) =< X_1, Y_2, S_1 \times S_2, \delta, \lambda >,$$

где $\delta(< s_1, s_2 >, x) =< \delta_1(s_1, x), \delta_2(s_2, \lambda_1(s_1, x)) >, \lambda(< s_1, s_2 >, x) = \lambda_2(s_2, \lambda_1(s_1, x))$, $x \in X_1, s_1 \in S_1, s_2 \in S_2$.

Если функция $g: {Y_1}^r \times {Y_2}^{p+1} \to Y_2$, а функция $f: {X_1}^{t+1} \to Y_1$, то КА $C'(M_f, M_g)$ с памятью порядка *(p + t,r)* определяется так:

$$y(i) = g\left(y(i-1), \dots, y(i-r), f\left(x(i), \dots, x(i-t)\right), \dots, f\left(x(i-p), \dots, x(i-p-t)\right)\right)$$
$$= g'\left(y(i-1), \dots, y(i-r), x(i), \dots, x(i-p-t)\right), i = 0,1, \dots$$

Конечно-автоматная криптосистема на основе DES оперирует КА с такими же характеристиками, что и в криптосистеме FAPKC.

Криптосистема Домёси (P. Dömösi) схожа с криптосистемами, построенными на основе КА Мили, тем, что для шифрования и дешифрования использует ключевой автомат. Ключевой автомат представляет собой матрицу перехода перестановочного автомата без выхода. Нужно отметить, что для дешифрования используется обратный ключевой автомат. P. Dömösi спроектировал симметричную криптосистему для поточного шифрования, основанную на Рабин-Скотта модели КА. Для блочного шифрования нашли своё применение произведения автоматов Глушкова (перестановочные автоматы без выхода) [18].

Заметим, что для *обратимости* автомата необходимо и достаточно, чтобы в его табличном представлении в каждой строке таблицы переходов все состояния были различны, т.е. автомат должен быть перестановочным. Это важное свойство, которое обеспечивает однозначность зашифрованного текста для любого открытого текста. Для безопасности предполагаем, что все столбцы таблицы переходов образуют перестановку набора состояний.

Как известно, дешифрование – это обратная функция к шифрованию, соответственно необходимо определить понятие обратного автомата без выхода.

Автомат $A^{-1} = < X, Q, \delta^{-1} >$, с функцией переходов $\delta^{-1}(b, x) = a$, где $a, b \in Q, x \in X$ называется *обратным* к автомату $A = < X, Q, \delta >$ тогда и только тогда, когда $\delta\ (a, x)=b$.

Тогда для $\forall a, b \in Q\ (a \neq b)$ и для $\forall x \in X^*$ выполняется равенство $A^{-1}\big(A(x)\big) = x$ [19].

Криптосистема, предложенная Лакшми (Lakshmi), использует автоматы Мили/Мура и рекурсивную функцию. КА является компонентом данной системы и входит в состав секретного ключа. Он предлагает использовать такие рекурсивные функции как рекуррентная матрица, производящая функция и граф, для которых определяется обратимость [20].

Рекуррентная матрица - это квадратная матрица порядка n, n> 0, элементы которой взяты из рекуррентного соотношения, например, это могут быть числа Фибоначчи. Данная матрица должна быть обязательно *невырожденной*.

Производящая функция $f(x)$ для рекуррентного отношения есть многочлен порядка (n-1) и имеет вид: $f(x) = a_0 + a_1 x + \ ... + a_{n-1} x^{n-1}$.

Обратный многочлен $F(x)$ к многочлену $f(x)$ является многочленом степени (n-1), если удовлетворяет следующему свойству: $f * F = 1$.

Пусть граф есть структура $G = (V, E, \varphi)$, где V – это непустое множество, элементы которого называются вершинами или узлами, E представляет собой набор из двух элементных подмножеств V, называемых ребрами, а φ – это функция с областью E и совместной областью $P_2(V)$.

Пусть функция $f(G)$ преобразует граф в число n, а функция $f(n)$ является обратной к функции $f(G)$. Матрица смежности A определяет граф G. Обратное неверно. Путём перестановки вершин группы G можно получить множество матриц смежности. Следовательно, должна быть предоставлена дополнительная информация для обеспечения инъективного свойства отображения.

4 Прикладные онтологии

Прикладные онтологии КАКГ охватывает широкую область знаний и предназначены в первую очередь для того, чтобы описать концептуальную модель конкретной задачи или приложения. Данный уровень описывает концепты, зависящие от верхних уровней онтологии. В статье приведён иллюстративный пример прикладной онтологии асимметричного криптографического алгоритма на основе КА – FAPKC. Данный алгоритм включает в себя большую часть описанных концептов. FAPKC с момента создания подвергся модификациям, которые представлены на рисунке 5. Нужно отметить, что общий алгоритм FAPKC остался неизменным, менялись виды используемых в криптосистеме автоматов.

Концепция конечно-автоматной криптосистемы с открытыми ключами заключается в том, что для шифрования открытого текста и верификации подписи используется открытый ключ, который состоит из последовательной композиции обратимых автоматов, в то время как обратные им автоматы входят в состав закрытого ключа, который используется для расшифровки и подписи сообщения. Считается, что без знания секретного ключа трудно инвертировать последовательность композиции автоматов [16].

Общая схема работы алгоритма FAPKC представлена на рисунке 6.

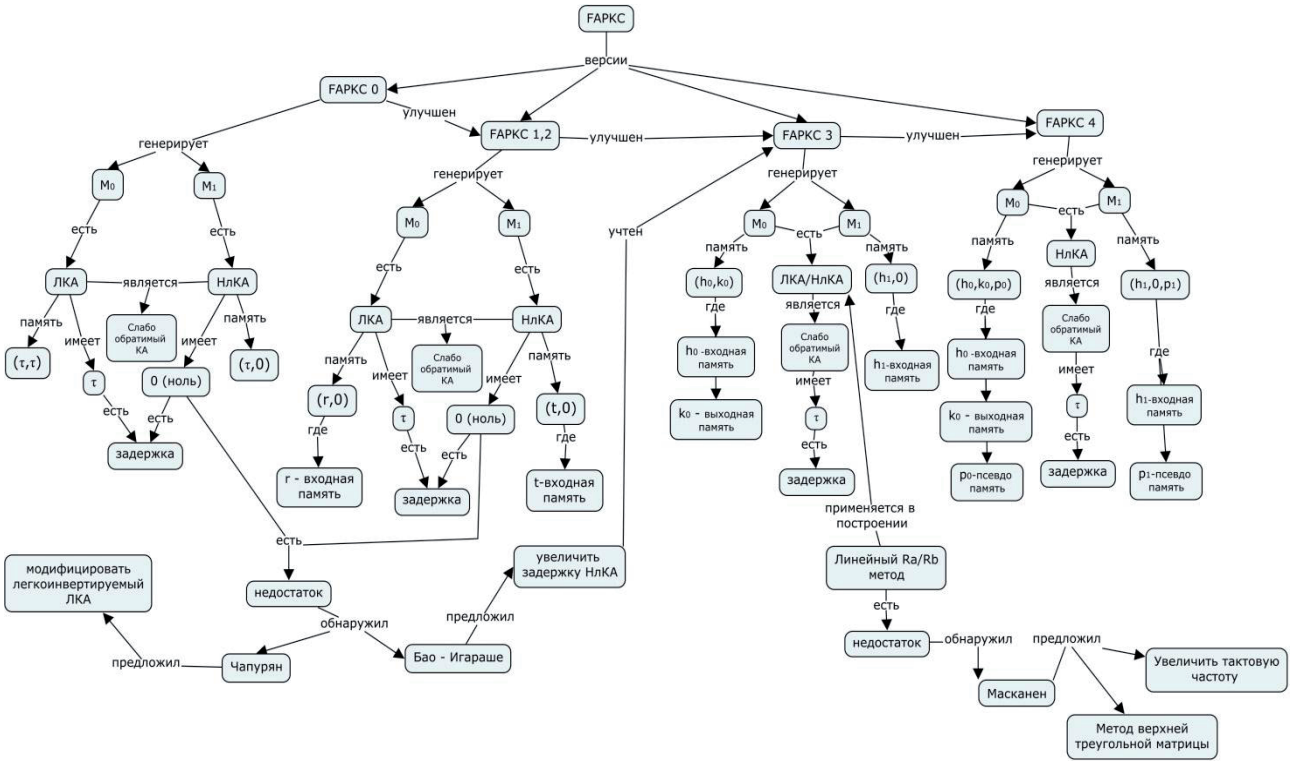

Рисунок 5 – Прикладная онтология FAPKC

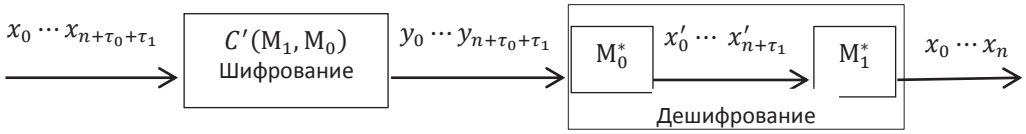

Рисунок 6 – Схема работы FAPKC

В отличие от теории чисел, где большое число можно всегда разложить на простые сомножители, для которых порядок их взаимного расположения в произведении не важен, в теории КА в композиции примитивных автоматов имеет значение как их набор, так и порядок взаимного расположения примитивных автоматов в композиции. Другими словами, композиция КА из примитивных автоматов не обладает свойством коммутативности. Поэтому разложение композиции КА на примитивные автоматы позволяет создавать сверхнадёжные системы защиты информации [21].

Общий алгоритм FAPKC.

В конечно-автоматной криптосистеме с открытыми ключами пользователь выбирает открытый и закрытый ключи по следующему алгоритму.

1) генерируются обратимый автомат M_0 = <X,Y,S_0,δ_0,λ_0> с памятью порядка (r_0, t_0) и обратимый к нему автомат M_0^* = <Y,X,S_0^*,δ_0^* ,λ_0^*> с памятью порядка (r_0^*, t_0^*) и с задержкой τ_0.
2) генерируется обратимый автомат M_1 = <X,X,S_1,δ_1,λ_1> с входной памятью порядка - h_1 и обратный к нему автомат M_1^* = <X,X,S_1^*,δ_1^* ,λ_1^*> памятью порядка (τ_1, h_1) с задержкой τ_1.
3) строится композиция автоматов M_1 и M_0 $C'(M_1, M_0)$ = <X,Y,S,δ,λ>.
4) определяется τ. Выбирается произвольное состояние s_e автомата $C'(M_1, M_0)$, которое и будет началом шифрования. Определяются части, необходимые для дешифрования: $s_{1,d}^{out}$ и $s_{0,d}^{out}$, для подписи и проверки: s_v^{out} , s_v^{in} , $s_{0,s}$, $s_{1,s}$.
5) открытый ключ пользователя состоит из $\{C'(M_1, M_0),\ s_v^{out}, s_v^{in}, s_e, \tau_0 + \tau_1\}$. Закрытый ключ пользователя состоит из $\{M_0^*, M_1^*, s_{0,s}, s_{1,s}, s_{1,d}^{out}, s_{0,d}^{out}, \tau_0, \tau_1\}$.

Шифрование: К концу заданного открытого текста $x_0 \cdots x_n$ добавляются произвольные символы длины $x_{n+1} \cdots x_{n+\tau_0+\tau_1}$и вычисляется шифртекст по открытому ключу, $y_0 \cdots y_{n+\tau_0+\tau_1} = \lambda(s_e, x_0 \cdots x_{n+\tau_0+\tau_1})$.

Дешифрование: Открытый текст получают в два этапа. Вначале вычисляется $x'_0 \cdots x'_{n+\tau_1} = \lambda_0^*(< x_{-1,e}, \dots, x_{-h_0,e}, y_{\tau_0-1}, \dots, y_0, y_{-1,e}, \dots, y_{-k_0,e} >, y_{\tau_0} \cdots y_{n+\tau_0+\tau_1})$.

Затем находят $x_0 \cdots x_n = \lambda_1^*(< x_{-1,e}, \dots, x_{-h_1,e}, x'_{\tau_1-1}, \dots, x'_0 >, x'_{\tau_1}, \dots, x'_{n+\tau_1})$.

Подпись: К концу сообщения $y_0 \cdots y_n$ добавляются произвольные символы длины $y_{n+1} \cdots y_{n+\tau_0+\tau_1}$. Затем вычисляется подпись $x_0 \cdots x_{n+\tau_0+\tau_1} = \lambda_1(s_{1,s}, \lambda_0^*(s_{0,s}, x_0 \cdots x_{n+\tau_0+\tau_1}))$, используя часть секретного ключа $M_0^*, M_1^*, s_{0,s}, s_{1,s}$.

Проверка: Проверка подлинности подписи сообщения $x_0 \cdots x_{n+\tau_0+\tau_1}$ проводится использованием части открытого ключа $C'(M_1, M_0)$, s_v^{out} и s_v^{in}. Вычисляется

$\lambda(< y_{-1,s}, \dots, y_{-t_0}, x_{\tau_0+\tau_1-1}, \dots, x_0, x_{-1,s}, \dots, x_{-r_0-r_1+\tau_0+\tau_1,s} >, x_{\tau_0+\tau_1} \dots x_{n+\tau_0+\tau_1})$,
которое должно совпадать с сообщением $y_0 \cdots y_n$.

В таблице 1 показаны характеристики версий криптосистемы FAPKC.

Таблица 1 – Характеристики криптосистемы FAPKC

FAPKC версии	**Вид автомата**	(r_0, t_0)	(r_0^*, t_0^*)	**Задержка**	**Формальное представление**
FAPKC0	M_0-линейный КА	(τ,τ)	(τ,0)	τ	$y(i) = \sum_{j=1}^{\tau} A_j\, y(i-j) + \sum_{j=0}^{\tau} B_j x'(i-j), i = 0,1,2, \dots$
	Нелинейная функция *f*	(r+1)		0	$f(v_0, \dots, v_r) \mid \forall v_1, \dots, v_r, f(v_0, \dots, v_r)$ − обратима от аргумента v_0
FAPKC1	M_0-линейный КА	(r,0)	(τ,r)	τ	$x'(i) = g\big(y'(i-r), \dots, y(i)\big), i = 0,1, \dots$
	M_1-нелинейный КА	(t,0)	(0,t)	0	$y'(i) = f\big(y'(i-t), \dots, y(i)\big), i = 0,1, \dots$
FAPKC2	M_0-линейный КА	(r,0)	(r,r)	r	$x'(i) = g\big(y'(i-r), \dots, y(i)\big), i = 0,1, \dots$
	M_1-нелинейный КА	(t,0)	(τ,r)	τ	$y'(i) = f\big(y'(i-t), \dots, y(i)\big), i = 0,1, \dots$
FAPKC1 (Bao, Igarashe)	M_0-линейный КА	(r,t)	(t+τ,r)	τ	$y(i) = \sum_{j=0}^{r} A_j\, x(i-j) + \sum_{j=1}^{t} B_j y(i-j), i = 0,1,2, \dots$
	M_1-нелинейный КА	(r,0)	(τ,r)	τ	$y(i) = \sum_{j=0}^{\tau} A_j\, x(i-j) + \sum_{j=1}^{\tau-1} B_j y(i-j), i = 0,1,2, \dots$
FAPKC3	M_0-линейный/ нелинейный КА	(h_0,k_0)	$(k_0+\tau_0, h_0)$	τ_0	$y(i) = \sum_{j=1}^{k_0} A_j\, y(i-j) + \sum_{j=0}^{h_0} B_j x(i-j), i = 0,1,2, \dots$ $y(i) = \sum_{j=1}^{k_0} A_j\, y(i-j) + \sum_{j=0}^{h_0} B_j x(i-j) + \sum_{j=0}^{h_0-\epsilon} B'_j s(x(i-j), \dots, x(i-j-\epsilon))$,
	M_1-нелинейный КА	$(h_1,0)$	(τ_1, h_0)	τ_1	$x'(i) = \sum_{j=0}^{h_1} F_j\, x(i-j) + \sum_{j=0}^{h_1-\epsilon} F'_j s(x(i-j), \dots, x(i-j-\epsilon)), i = 0,1,2, \dots$ где $s(x(i-j), \dots, x(i-j-\epsilon))$- нелинейная функция, а ϵ – маленькое положительное целое число.
FAPKC3 (Mes-kanen)	M_0-линейный	(h_0,k_0)	$(k_0+\tau_0, h_0)$	τ_0	$y(i) = \sum_{j=1}^{k_0} A_j\, y(i-j) + \sum_{j=0}^{h_0} B_j x(i-j) + \sum_{j=h_0+1}^{2h_0} B_{2h_0-j} x(i-j)$, *i=0,1,2,…*
	M_1-нелинейный КА	$(h_1,0)$	(τ_1, h_0)	τ_1	$x'(i) = \sum_{j=0}^{h_1} F_j\, x(i-j) + \sum_{j=0}^{h_1-\epsilon} F'_j s(x(i-j), \dots, x(i-j-\epsilon)), i = 0,1,2, \dots$
FAPKC4	M_0-линейный/ нелинейный КА	(h_0, k_0, p_0)	$(\tau_0 + k_0, h_0, p_0)$	τ_0	$y(i) = f\big(y(i-1), \dots, y(-k_0), u(i), \dots, u(i-p_0), x(i), \dots, x(-h_0)\big)$, $u(i+1) = g\big(y(i-1), \dots, y(-k_0), u(i), \dots, u(i-p_0), x(i), \dots, x(i-h_0)\big)$, *i* = 0,1, …
	M_1-нелинейный КА	$(h_1, 0, p_1)$	(τ_1, h_1, p_1)	τ_1	$y(i) = f\big(u(i), \dots, u(i-p_1), x(i), \dots, x(i-h_1)\big)$, $u(i+1) = g\big(u(i), \dots, u(i-p_1), x(i), \dots, x(i-h_1)\big)$, *i* = 0,1, …

В версии FAPKC0, приведённой в [22], открытый ключ содержит составной КА из обратимого линейного автомата с памятью порядка (τ, τ) и с задержкой τ и слабо обратимого нелинейного КА с входной памятью и с задержкой 0. Две другие схемы FAPKC1 и FAPKC2 приведены в [23], где открытый ключ для FAPKC1 содержит композицию двух КА: обратимый линейный автомат с входной памятью порядка τ и с задержкой τ, слабо обратимый нелинейный КА с входной памятью и с задержкой 0. В работе [24] доказано, что FAPKC1 небезопасен в шифровании и предлагается модификация с использованием квазилинейных КА. В [23] разработан метод генерации своего рода нелинейных слабо обратимых КА; затем две схемы, названные FAPKC3 и FAPKC4, были предложены в [25, 26]. Для версий FAPKC3 были предложены иные модификации в работе [17].

Заключение

Актуальность создания онтологии КАКГ обусловлена необходимостью в систематизации полученных знаний в криптографии. Цель предложенной онтологической модели - формирование наглядной когнитивной модели, которая отражает все основные концепты криптосистем, основанных на теории автоматов, и характер их связей. Данная модель может улучшить понимание такого рода криптосистем при планировании их реализации.

Для формирования онтологии КАКГ использована методология К-карт, которая обладает такими преимуществами как системность, единообразие, научность и когнитивность.

Структура области КАКГ рассматривается как сложно-структурированный объект, который получен путём интеграции двух самостоятельных областей - криптографии и теории автоматов. Использована четырёхуровневая онтологическая модель, включающая представление знаний – методологию К-карт, онтологии криптографии и теории автоматов, онтологию КАКГ, прикладные онтологии.

Предложенную онтологию можно использовать для решения таких задач:

- обеспечение общим понятийным и терминологическим аппаратом специалистов, интересующихся данной ПрО;
- создание интеллектуальных систем принятия решения в криптографической защите информации;
- организация эффективного поиска информации о КАКГ.

Список источников

[1] ***Гатченко, Н.А.*** Криптографическая защита информации / Н.А. Гатченко, А.С. Исаев, А.Д. Яковлев - СПб: НИУ ИТМО, 2012. -142 с.

[2] ***Сущевский, Д.Г.*** Современные криптосистемы и их особенности / Д.Г. Сущевский, О.В. Панченко, В.Н. Кугураков // Вестник технического университета. – 2015. – №11(18). – С.194-197.

[3] ***Мирзагитов, А.А.*** Методы разработки онтологии по информационной безопасности, основанные на прецедентном подходе / А.А. Мирзагитов, Д.Е. Пальчунов // Вестник Новосиб. гос. ун-та. Серия: Информационные технологии. – 2013. – №3(11). – С. 37-46.

[4] ***Cañas, A.J.*** CMAPTOOLS: a knowledge modeling and sharing environment / A.J. Cañas, G. Hill, R. Carff, N. Suri, J. Lott, G. Gómez, Th. C. Eskridge, M. Arroyo, R. Carvajal. – http://cmc.ihmc.us/papers/cmc2004-283.pdf.

[5] ***Gruber, T.R***. A Translation Approach to portable ontology specifications/ T.R. Gruber // Knowledge acquisition. – 1993. - №5 (2). – P. 199-220.

[6] ***Ивлеев, А.А.*** Онтология военных технологий: основы, структура, визуализация и применение (1 часть) / А.А. Ивлеев, В.Б. Артеменко // Вооружение и экономика. – 2011. - №4 (16). – С.35-52 - http://www.viek.ru/16/35-52.pdf

[7] ***Novak, J.D.*** The Theory Underlying Concept Maps and How to Construct and Use Them / J.D. Novak, A.J. Cañas. - http://cmap.ihmc.us/docs/theory-of-concept-maps.

[8] ***Гаврилова, Т.А.*** Анализ ошибок студентов при визуальном структурировании знаний / Т.А. Гаврилова, В.А. Онуфриев // Компьютерные инструменты в образовании. – 2016. – № 6. – С.42-54 - http://ipo.spb.ru/journal.
[9] ***Бачурина, Е.П.*** Стратегия онтологического инжиниринга при управлении знаниями в области ЧС / Е.П. Бачурина // Тез. VI Всерос. науч.-техн. конф. студентов, аспирантов и молодых ученых «Молодежь и наука». – Красноярск, 2010. – С. 304-308.
[10] ***Муромский, А.А***. Использование онтологического подхода для защиты данных при их пересылке и архивации / А.А. Муромский, Н.П. Тучкова // Онтология проектирования. – 2016. – Т. 6, №2(20). - С. 136-148. – DOI: 10.18287/2223-9537-2016-6-2-136-148.
[11] ***Саломаа, А.*** Криптография с открытым ключом / А. Саломаа. Перевод с английского И.А. Вихлянцева под редакцией А.Е. Андреева и А.А. Болотова – М.: Мир, 1995. - 318 с.
[12] ***Гуренко, В.В.*** Введение в теорию автоматов / В.В. Гуренко. – М.: МГТУ им. Н.Э. Баумана, 2013. – 62 с.
[13] ***Шарипбай, А.А.*** Теория языков и автоматов / А.А. Шарипбай. – Алматы, Эверо, 2015. - 207 с.
[14] ***Трахтенброт, Б.А.*** Конечные автоматы (поведение и синтез) / Б.А. Трахтенброт, Я.М. Барздинь. – Москва, Наука, 1970. – 400 с.
[15] ***Шарипбай, А.А.*** Автоматные модели в криптографии / А.А. Шарипбай // Вестник КазНУ. Серия: математика, механика, информатика. – 2016. - №3/1 (90). – С.96-104.
[16] ***Tao, R.J.*** Finite Automata and Application to Cryptography/ R.J. Tao. – Tsinghua University Press, 2009. – 406 p.
[17] ***Meskanen, T***. On finite automaton public key cryptosystems / T. Meskanen // TUCS Technical Report. – Turku, 2001. – No.408. – 46 p.
[18] ***Dömösi, P.A.*** Novel Cryptosystem Based on Gluskov Product of Automata / P. Dömösi, G. Horváth // Acta Cybernetica. – 2015. – P.359–371.
[19] ***Dömösi, P.A.*** Novel Cryptosystem Based on Finite Automata Without Outputs / P. Dömösi // Automata, Formal Languages and Algebraic Systems. – 2010. – P.23-32.
[20] ***Gandhi, B.K***. Cryptographic Scheme for Digital Signals using Finite State Machines / B.K. Gandhi, A. Ch. Sekhar, S.S. Lakshmi // International Journal of Computer Applications. – 2011. - №6 (29). – P. 61-63.
[21] ***Шахметова, Г.Б.*** Применение конечных автоматов для разработки асимметричных шифров / Г.Б. Шахметова, А.А. Шарипбай, Ж.С. Сауханова, Г.Ж. Исабаева // Труды V Международной научно-практической конференции «Интеллектуальные информационные и коммуникационные технологии – средство осуществления третьей индустриальной революции в свете стратегии «КАЗАХСТАН-2050». – 2018. – С.286-289.
[22] ***Tao, R.*** A finite automaton public key cryptosystem and digital signatures [китайский]/ R. Tao, Sh. Chen // Chinese Journal of Computers. – 1985. Vol.8(6). – P. 401-409.
[23] ***Tao, R***. Two varieties of finite automaton public key cryptosystem and digital signatures / R. Tao, Sh. Chen // Journal of computer science and technology. – 1986. Vol. 1(1). – P.9-18.
[24] ***Bao, F.***, Break finite automata public key cryptosystem / F. Bao, Y. Igarashi. // In International Colloquiumon Automata, Languages, and Programming, Springer Berlin Heidelberg. – Berlin, 1995. – P.147-158.
[25] ***Tao, R.*** FAPKC3: a new finite automaton public key cryptosystem / R. Tao, Sh. Chen, X. Chen // Journal of Computer science and Technology. – 1997. – Vol.12(4). – P.289-305.
[26] ***Tao, R.*** The generalization of public key cryptosystem FAPKC4 / R. Tao, Sh. Chen // Chinese science bulletin. – Chinese, 1999. – Vol.44(9). – P.784-790.

ONTOLOGY OF FINITE-AUTOMATION CRYPTOGRAPHY

A.A. Sharipbay[1], Zh.S. Saukhanova[2], G.B. Shakhmetova[3], M.S. Saukhanova[4]

Eurasian national university named after L.N. Gumilyov, Astana, Kazakhstan
[1] *sharalt@mail.ru,* [2] *saukhanova@mail.ru,* [3] *shakhmetova.gb@gmail.com,* [4] *m.saukhanova@mail.ru*

Abstract

Today, the improvement of methods for protecting information is an urgent task, therefore, the authors of the article are interested in using alternative methods of developing more robust and efficient public-key cryptosystems. Finite automata are taken as such a model. To systematize knowledge in the field of finite-state cryptography, it was decided to use ontology. This paper discusses the construction of an ontological model of finite-automaton cryptography. The proposed ontological model will have four main levels: the ontology of knowledge representation, the ontology of the top

level, the domain ontology and practical ontologies. The methodology of conceptual maps was taken as the ontology of knowledge representation. The ontology of the top level contains basic information about cryptography and automata theory, the domain ontology describes directly the finite automaton cryptography. As an example of practical ontology, a public-key cryptosystem based on finite automata was considered. The presented ontology is modeled for the first time and gives a clear understanding of the use of finite automata in cryptography, systematizes the information obtained in the course of the research on this subject area, is a prerequisite in the further development of cryptosystems based on the theory of automata.

Key words: *ontology, conceptual map, finite automata, cryptography*.

Citation: *Sharipbay AA, Saukhanova ZhS, Shakhmetova GB, Saukhanova MS.* Ontology of finite-automation cryptography [In Russian]. *Ontology of designing*. 2019. 9(1): 36-49. – DOI: 10.18287/2223-9537-2019-9-1-36-49.

References

[1] ***Gatchenko NA, Isaev AS, Yakovlev AD.*** Cryptographic protection of information: textbook [In Russian]. Petersburg: NRU ITMO; 2012.

[2] ***Suschevsky DG, Panchenko OV, Kugurakov VN.*** Modern cryptosystems and their features [In Russian]. Bulletin of the Technical University 2015; 11(18): 194-197.

[3] ***Mirzagitov AA, Palchunov DE.*** Methods for developing ontologies for information security based on a case-law approach [In Russian] Bulletin of Novosib. state un-that. Series: Information Technology 2013; 3(11): 37-46.

[4] ***Cañas AJ, Hill G, Carff R, Suri N, Lott J, Gómez G, Eskridge ThC, Arroyo M, Carvajal R***. CMAPTOOLS: a knowledge modeling and sharing environment. - http://cmc.ihmc.us/papers/cmc2004-283.pdf.

[5] ***Gruber TR.*** A Translation Approach to portable ontology specifications: Proc. of Knowledge acquisition 1993; 5(2): 199-220.

[6] ***Ivleev AA, Artemenko VB.*** Ontology of military technologies: fundamentals, structure, visualization and application (1 part) [In Russian] Armament and economy 2011; 4(16): 35-52. - http://www.viek.ru/16/35-52.pdf.

[7] ***Novak JD, Cañas AJ.*** The Theory Underlying Concept Maps and How to Construct and Use Them - http://cmap.ihmc.us/docs/theory-of-concept-maps.

[8] ***Gavrilova TA, Onufriev VA.*** Analysis of students' mistakes in the visual structuring of knowledge [In Russian] Computer tools in education 2016; 6: 42-54. - http://ipo.spb.ru/journal.

[9] ***Bachurina EP.*** Strategy of ontological engineering in knowledge management in the field of emergency situations [In Russian]. Thesis of VI All-Russian scientific and technical conf. students, graduate students and young scientists "Youth and Science." – Krasnoyarsk; 2010: 304-308.

[10] ***Muromskii AA, Tuchkova NP.*** Ontological approach to the data protection for their transfer and archiving [In Russian] *Ontology of designing.* 2016; 2(20): 136-148. DOI: 10.18287/2223-9537-2016-6-2-136-148.

[11] ***Salomaa A.*** Public- key Cryptography. - Springer-Verlag; 1996.

[12] ***Gurenko VV.*** Introduction to Automata Theory [In Russian]. - Moscow: Moscow State Technical University named after NE Bauman; 2013.

[13] ***Sharipbay AA.*** Theory of languages and automata [In Russian]. - Almaty, Evero; 2015.

[14] ***Trakhtenbrot BA., Barzdin YaM.*** State machine (behavior and synthesis) [In Russian]. – Moscow, Nauka; 1970.

[15] ***Sharipbay AA.*** Automata models in cryptography [In Russian] KazNU Bulletin. Mathematics, Mechanics, Computer Science Series. 2016; 3/1(90): 94-104.

[16] ***Tao RJ.*** Finite Automata and Application to Cryptography. – Tsinghua University Press; 2009.

[17] ***Meskanen T.*** On finite automaton public key cryptosystems. *TUCS Technical Report*. – Turku; 2001.

[18] ***Dömösi P, Horváth G.*** A Novel Cryptosystem Based on Gluskov Product of Automata. *Acta Cybernetica*; 2015: 359–371.

[19] ***Dömösi P.*** A Novel Cryptosystem Based on Finite Automata Without Outputs. *Automata, Formal Languages and Algebraic Systems*; 2010: 23-32.

[20] ***Gandhi BK, Sekhar ACh, Lakshmi SS***. Cryptographic Scheme for Digital Signals using Finite State Machines. *International Journal of Computer Applications.* 2011; 6 (29): 61-63.

[21] ***Shakhmetova GB, Sharipby AA, Saukhanova ZhS, Isabaeva GZh.*** The use of finite automata for the development of asymmetric ciphers [In Russian]. Proceedings of the V International Scientific and Practical Conference "Intelligent Information and Communication Technologies - the medium of the third industrial revolution in the light of the strategy" KAZAKHSTAN-2050 "; 2018: 286-289.

[22] ***Tao R, Chen Sh.*** A finite automaton public key cryptosystem and digital signatures [In Chinese]. Chinese Journal of Computers 1985; 8(6): 401-409.

[23] ***Tao R, Chen Sh.*** Two varieties of finite automaton public key cryptosystem and digital signatures. Journal of computer science and technology 1986; 1(1): 9-18.
[24] ***Bao F, Igarashi Y.*** Break finite automata public key cryptosystem. In International Colloquiumon Automata, Languages, and Programming, Springer Berlin Heidelberg (Berlin, 1995); 1995: 147-158.
[25] ***Tao R, Chen Sh, Chen X***. FAPKC3: a new finite automaton public key cryptosystem. *Journal of Computer science and Technology*. 1997; 12(4): 289-305.
[26] ***Tao R, Chen Sh***. The generalization of public key cryptosystem FAPKC4. *Chinese science bulletin*. 1999; 44(9): 784-790.

Сведения об авторах

Шарипбай Алтынбек Амирович, 1952 г. рождения. К.ф.-м.н., д.т.н., профессор по группе специальностей «Информатика, вычислительная техника и управление», академик «Международной Академии информатизации», академик «Академии педагогических наук Республики Казахстан». Профессор кафедры «Информатика и информационная безопасность», директор НИИ «Искусственный интеллект» Евразийского национального университета им. Л.Н. Гумилева (ЕНУ). В списке научных трудов более 200 работ в области искусственного интеллекта, компьютерной лингвистики, информационной безопасности.

Altynbek Amirovich Sharipbay, born in 1952. Candidate of Physical and Mathematical Sciences, Doctor of Technical Sciences, Professor in the group of specialties "Informatics, computer engineering and control", academician of the "International Academy of Informatization", academician of the "Academy of Pedagogical Sciences of the Republic of Kazakhstan". Professor of the Department "Informatics and Information Security", Director of the Research Institute "Artificial Intelligence" of the Eurasian National University. L.N. Gumilyov. In the list of scientific works more than 200 works in the field of artificial intelligence, computational linguistics, information security.

Сауханова Жанат Сергазиевна, 1964 г. рождения. Окончила Санкт-Петербургский государственный университет, факультет прикладной математики - процессов управления. К.ф.-м.н., доцент кафедры «Информатика и информационная безопасность» ЕНУ им. Л.Н. Гумилева. В списке научных трудов более 50 работ в области программирования, больших данных, информационной безопасности.

Zhanat Sergazievna Saukhanova, born in 1964. She graduated from St. Petersburg State University, faculty of applied mathematics - management processes. Candidate of Physical and Mathematical Sciences, Associate Professor of the Department "Informatics and Information Security" of the Eurasian National University. L.N. Gumilyov. In the list of scientific works more than 50 works in the field of programming, big data, information security.

Шахметова Гульмира Балтабаевна, 1982 г. рождения. Окончила магистратуру ЕНУ им. Л.Н. Гумилева по специальности «Информатика». Является докторантом 2 курса специальности «Информатика» ЕНУ им. Л.Н. Гумилева. В списке научных трудов более 15 статей в области теории автоматов и формальных языков, информационной безопасности, ИКТ в образовании.

Gulmira Baltabaevna Shakhmetova, born in 1982. She graduated from the magistracy of the Eurasian National University. L.N. Gumilyov specialty "Computer Science". She is a PhD student of the 2 course of the specialty "Computer Science" of the ENU L.N. Gumilyov. The list of scientific works includes more than 15 articles in the field of automata theory and formal languages, information security, ICT in education.

Сауханова Магрипа Сергазиевна, 1962 г. рождения. Окончила магистратуру ЕНУ им. Л.Н. Гумилева по специальности «Информатика». Старший преподаватель кафедры «Вычислительная техника и программное обеспечение» Евразийского национального университета им. Л.Н. Гумилева. В списке научных трудов более 20 статей в области ИКТ в образовании, автоматного программирования, информационной безопасности.

Magripa Sergazievna Saukhanova, born in 1962. She graduated from the magistracy of the Eurasian National University L.N. Gumilyov specialty "Informatics". She is a senior lecturer in the department of "Computing equipment and software" of the Eurasian National University L.N. Gumilyov. In the list of scientific works more than 20 articles in the field of ICT in education, automated programming, information security.