Выходит с 2006 г.

СИСТЕМЫ ВЫСОКОЙ ДОСТУПНОСТИ

№ 4, т. 14, 2018

Highly available systems

Журнал включен в перечень ВАК

Журнал издается под научно-методическим руководством Федерального исследовательского центра «Информатика и управление» Российской академии наук.

СОДЕРЖАНИЕ

CONTENTS

Все статьи, представленные в данном выпуске журнала, соответствуют номенклатуре специальностей научных работников (Приказ Минобрнауки РФ от 11.08.2009 № 294) по отраслям технических наук.

Journal «Sistemy' vy'sokoj dostupnosti» («Highly available systems»).
The journal covers scientific and engineering problems of ensuring confidentiality, availability, and integrity for the class of information-telecommunication systems of high availability (HA ITS), which contain such critical technologies of development

Необходимую информацию о журнале и полный список опубликованных статей, а также аннотации к ним Вы найдете на нашем сайте http://www.radiotec.ru

Учредитель: ООО «Издательство «Радиотехника».

Лицензия № 065229. Свидетельства о регистрации ПИ № ФС 77-25037 от 12 июля 2006 г.
Сдано в набор 18.10.2018 г. Подписано в печать 22.11.2018 г.
Печ. л. 10. Тираж 400 экз. Изд. № 117.
Адрес Издательства «Радиотехника»: 107031, Москва, К-31, Кузнецкий мост, д. 20/6. Тел./факс 621-4837.
E-mail: info@radiotec.ru
http: // www. radiotec.ru /

Дизайн и допечатная подготовка ООО «САЙНС-ПРЕСС».
Отпечатано с предоставленных готовых файлов в полиграфическом центре ФГУП Издательство «Известия».
127254, ул. Добролюбова, д. 6. Контактный телефон (495) 650-38-80. izv-udprf.ru. Заказ №.

ISSN 2072-9472

К читателям

DOI: j20729472-201804-01

В первой части настоящего выпуска журнала «Системы высокой доступности» публикуются не вошедшие в предыдущий третий выпуск материалы семи докладов научного форума – VI Международной научно-практической конференции «Управление информационной безопасностью в современном обществе», которая состоялась в Москве в июне 2018 г. в Высшей школе экономики. Публикуемые материалы научных докладов в полной мере соответствуют требованиям и духу нашего журнала.

Главный редактор журнала
«Системы высокой доступности»,
академик Академии криптографии РФ ***В.И. Будзко***

Состоявшаяся 5−7 июня 2018 г. конференция «Управление информационной безопасностью в современном обществе» собрала более 300 специалистов в области обеспечения безопасности информационно-аналитических систем. На конференции были рассмотрены актуальные направления развития и представлены новейшие разработки ряда ведущих фирм России. Большой интерес вызвали обсуждения проблем управления процессами создания и эксплуатации отечественных операционных систем и компонент коммуникационного оборудования, создаваемого в рамках импортозамещения. Можно констатировать, что обмен мнениями и научный подход к проблемам импортозамещения позволил в определенной степени консолидировать усилия различных разработчиков, более четко сформулировать области применения разных изделий, а в ряде случаев устранить недопонимание функциональных особенностей разработок.

На пленарном заседании выступали ведущие ученые в области создания аналитических информационных систем (АИС), выделившие основные перспективные направления развития отрасли. Обширные доклады содержали полезную информацию как для ученых и специалистов-разработчиков, так и для преподавателей и студентов различных учебных заведений.

Выражаю благодарность всем участникам конференции за активное и заинтересованное обсуждение проблем. Успешное проведение конференции было бы невозможно без поддержки руководства Высшей школы экономики и Школы бизнес-информатики профессора С.В. Мальцевой.

Член редколлегии журнала
«Системы высокой доступности»,
председатель Программного комитета конференции,
академик Академии криптографии РФ ***А.П. Баранов***

УДК 621.391(075.8)

Метод многоступенчатого гомоморфизма шифров с обратной связью по выходу на примере шифра IA

А.В. Бабаш – д.ф.-м.н., профессор, НИУ ВШЭ (Москва)
E-mail: avbabash@hse.ru

Проведен криптоанализ усложненного варианта шифра IA. Использована атака «многоступенчатого гомоморфизма конечного автомата». Оценена сложность атаки.

Ключевые слова: *шифр, атака, гомоморфизм автомата.*

A cryptanalysis of the complicated version of cipher IA is carried out. The attack of the «multistage homomorphism of the finite automaton» is used. The complexity of the attack is assessed.

Keywords: *cipher, attack, homomorphism of an automaton.*

DOI: 10.18127/j20729472-201804-02

Ц е л ь р а б о т ы – провести криптоанализ усложненного варианта шифра IA.

Описание IA

Шифр IA (Indirection, Addition) предложил Дженкинс в 1996 г. Состояниями генератора псевдослучайных чисел IA являются тройки (G,Q,i), где $G: Z_m \to Z_{2^K}$ – произвольное отображение кольца вычетов по модулю $m = 2^n$ в кольцо вычетов по модулю 2^K; Q – произвольный элемент кольца вычетов Z_{2^K}, $K = 2n + \Delta$, $\Delta \geq 0$, $i \in Z_m$. Начальные состояния IA имеют вид $(G_1, Q_1 = 0, i_1 = 0)$.

В каждый момент времени $t \in [1;\infty)$ в IA происходит переход из состояния $(G_{t-1}, Q_{t-1}, i_{t-1})$ в новое состояние (G_t, Q_t, i_t) и выработка нового элемента Q_t выходной последовательности. При этом выполняются следующие действия:

$$i_t = i_{t-1} + 1 \mod(m),$$

$$G_t[i_t] = G_{t-1}[G_{t-1}[i_t](\mathrm{mod}\, m)] + Q_{t-1}, \quad Q_t = G_t[(G_t[i_t] >> n)(\mathrm{mod}\, m)] + G_{t-1}[i_t], \quad z_t = Q_t, \qquad (1), (2), (3)$$

где $G_t[j]$ – образ элемента j для отображения G_t; «+» – операция сложения по модулю 2^K; $(G[i_t] >> n)$ – представление $G[i_t]$ в двоичном виде с последующим сдвигом вправо на n разрядов, затем перевод полученного двоичного вектора в элемент Z_m; z_t – выходная последовательность.

Шифрование t-го знака открытого текста $a_t \in Z_K$ проводится сложением по модулю 2 знаков a_t открытого текста и z_t, представленных в виде двоичных векторов длины K.

Построение автоматной модели усложненного IA

Рассмотрим следующую модернизацию IA, заменив равенства (2) и (3) на выражения

$$Q_t = G_t[(G_t[i_t] >> n + \Delta)] + G_{t-1}[i_t], \qquad (4)$$

$$y_t = Q_t, F_t(G_t) \text{ при нечетном } t \text{ и } y_t = F_t(S_t), Q_t \text{ при четном } t, \qquad (5)$$

где $t \in \{1, 2, \ldots, m-1, 0\}$.

Для краткого определения значения функции $F_t(S_t)$ введем вспомогательную произвольную двоичную функцию $f_t\left[v(1), \ldots, v(m-1), v(0)\right]$ в форме многочлена Жегалкина. Она определена через операции сложения по модулю 2 и конъюнкции переменных. Заменим переменные $v(j)$ на $G_t[j]$, а опера-

ции сложения по модулю 2 и конъюнкции переменных на операции сложения и умножения переменных по mod2^K.

Постановка задачи. Задача состоит в нахождении начального состояния G_1 по входной последовательности 1, 2, …, m−1, 0, … периода m и выходной последовательности y_t, $t \in [1, L]$ модернизированного шифра IA.

Первая автоматная модель модернизированного IA

Обозначим через $B_k^{ia} = \left[X, \Sigma_{2^k}^m \times Z_{2^k}, Y, (H_x,\ x \in Z_m), (F_x,\ x \in Z_m) \right]$ конечный автомат, где $X = Z_m$ – входной алфавит; $Y = Z_{2^k}$ – выходной алфавит; $\Sigma_{2^k}^m \times Z_{2^k}$ – множество состояний; $\Sigma_{2^k}^m$ – множество всех отображений $G : Z_m \to Z_{2^k}$; $G[j]$ – образ элемента $j \in Z_m$; $(H_x,\ x \in Z_m)$ – семейство частичных функций переходов $H_x : \Sigma_{2^k}^m \times Z_{2^k} \to \Sigma_{2^k}^m \times Z_{2^k}$; $(F_x,\ x \in Z_m)$ – семейство частичных функций выхода $F_x : \Sigma_{2^k}^m \times Z_{2^k} \to Z_{2^k}$. При входном символе $x_t \in Z_m$ и состоянии (S_t, Q_t) в момент времени $t \in \{1, 2, \ldots\}$ $H_{x_t}(G_t, Q_t) = (G_{t+1}, Q_{t+1})$, $F_{x_t}(G_t, Q_t) = y_t$, где $G_{t+1}[x_t] = G_t[G_t[x_t](\mathrm{mod}\, m)] + Q_t$.

Значение Q_{t+1} вычисляется по формуле

$$Q_{t+1} = G_{t+1}[(G_{t+1}[x_t] >> n + \Delta)(\mathrm{mod}\, m)] + G_t[x_t], \tag{6}$$

а y_t определено в (5).

Отметим, что значения $G_{t+1}[j]$ и $G_t[j]$ отображений G_{t+1} и G_t совпадают на всех элементах $j \neq x_t$ множества Z_m, а операции «+» и «$>> n + \Delta$» введены ранее. Корректность записи (6) следует из того, что при фиксации $x \in Z_m$ отображение G_t является значением функции от Q_{t-1} и G_{t-1}.

Формулировка задачи в терминах первой автоматной модели усложненного IA. Задача состоит в поиске решения (g_1, q_1) уравнения

$$B_k^{ia}\left[(G_1, q_1), x_1, x_2, \ldots, x_L\right] = y_1 y_2 \ldots y_L \tag{7}$$

при известных последовательностях $x_1, x_2, \ldots, x_L$ и $y_1 y_2 \ldots y_L$.

Вторая автоматная модель усложненного IA

Автомат B_k^{ia} находится под наблюдением, а именно: дополнительно известна последовательность состояний $q_1 q_2 \ldots q_L$ второй компоненты в последовательности состояний $(g_1, q_1)(g_2, q_2)\ldots(g_L, q_L)$, которая соответствует начальному состоянию $(G_1, q_1) \in \Sigma_{2^k}^m \times Z_{2^k}$ и входному слову $x_1 x_2 \ldots x_L \in Z_{2^k}$.

В качестве второй автоматной модели усложненного IA используем автомат под наблюдением HB_K^{ia} со следующими параметрами: $X \times Z_{2^K}$ – входной алфавит; $\Sigma_{2^K}^m$ – множество состояний; $Y = Z_{2^K}$ – выходной алфавит; $(H_{x,Q}^1, x \in X, Q \in Z_{2^K})$ – семейство частичных функций переходов автомата, $H_{x_t,Q_t}^1(G_t) = G_{t+1}$, где $G_{t+1}[j] = G_t[j]$ при всех $j \in Z_m, j \neq x$, а при $j = x_t$ имеет место равенство $G_{t+1}[x_t] = G_t[G_t[x_t](\mathrm{mod}\, m)] + Q_t$; $(F_{x,Q}^1, x \in X, Q \in Z_{2^K})$ – семейство частичных функций выходов автомата, $F_{x_t,Q_t}^1(G_t) = Q_t$.

Поставленная выше задача сводится к нахождению начальной компоненты G_1 при известной входной последовательности $\begin{pmatrix} x_1 \\ Q_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ Q_2 \end{pmatrix}, \ldots, \begin{pmatrix} x_L \\ Q_L \end{pmatrix}$ и известной выходной последовательности $y_1 y_2 \ldots y_L$:

$$HB_K^{ia}\left[G_1,\binom{x_1}{Q_1}\binom{x_2}{Q_2}\dots\binom{x_L}{Q_L}\right]=y_1y_2\dots y_L,$$

где $x(1)x(2)\dots x(m-1)x(0)\dots=12\dots(m-1)0\dots$ – периодическая последовательность периода m.

Метод многоступенчатого гомоморфизма для автоматной модели под наблюдением шифра IA

В данном разделе автомат $HB_K^{ia}=\left[X\times Z_{2^K},\Sigma_{2^K}^m,Y,(H_{x,Q}^1,x\in X,Q\in Z_{2^K}),(F_{x,Q}^1,x\in X,Q\in Z_{2^K})\right]$ будем использовать в качестве автоматной модели IA. Автоматы HB_k^{ia} будут использованы как вспомогательные автоматы. В случае необходимости отображение $g\in\Sigma_{2^k}^m$ будем записывать в виде $g=\binom{j}{g[j]}_{2^k}^m$, а при $k=K$ в виде $G=\binom{j}{G[j]}_{2^k}^m$.

Главной задачей данного раздела является нахождение решения G_1 уравнения

$$HB_K^{ia}(G_1,x_1,x_2,\dots,x_L)=y_1y_2\dots y_L \tag{8}$$

при известных последовательностях $x_1,x_2,\dots,x_L$ и $y_1y_2\dots y_L$.

Для $k\in\{K,K-1,\dots,n+1\}$ определим отображения:

$$\psi_k:X\times Z_{2^k}\to X\times Z_{2^{k-1}},\ \psi_k(x,q)=(x,q(\mathrm{mod}2^{k-1}),$$

$$\varphi_k:\Sigma_{2^k}^m\to\Sigma_{2^{k-1}}^m,\ \varphi_k\left(\binom{j}{g[j]}_{2^k}^m\right)=\binom{j}{g[j]\bmod 2^{k-1}}_{2^{k-1}}^m,$$

$$\chi_k:Z_{2^k}\to Z_{2^{k-1}},\ \chi_k(q)=q\bmod 2^{k-1}.$$

Теорема 1. *Тройка отображений* $(\psi_k,\varphi_k,\chi_k)$, $k\in\{K,K-1,\dots,n+1\}$ *является гомоморфизмом автомата* HB_k^{ia} *на автомат* HB_{k-1}^{ia}.

Доказательство. Для доказательства теоремы 1 достаточно доказать ее утверждение для $k=K$. Надо доказать, что

$$\varphi_K H_{x,Q_{t-1}}(G_{t-1})=h_{\psi_k(x,Q_{t-1})}\left[\varphi_K(G_{t-1})\right]=h_{x,q_{t-1}}\varphi_K(G_{t-1}), \tag{9}$$

где $H_{x,Q_{t-1}}(G_{t-1})=G_t$.

Равенство $\chi_k(Q_{t-1})=Q_{t-1}\bmod 2^{k-1}=q_{t-1}$ очевидно. Исследуем левую часть равенства (9):

$$\varphi_K H_{x,Q_{t-1}}(G_{t-1})=\varphi_K G_t=\varphi_K\left(\binom{j}{G_t[j]}_{2^K}^m\right),$$

где $G_t[j]=G_{t-1}[j]$ при $j\neq x$, а $G_t[x]=(G_{t-1}[G_{t-1}[x](\mathrm{mod}\,m)]+Q_{t-1})$.

Далее $G_t[j]\bmod 2^{K-1}=G_{t-1}[j]\bmod 2^{K-1}$, $j\neq x$ и при $j=x$

$$G_t[x]\bmod 2^{K-1}=(G_{t-1}[G_{t-1}[x](\mathrm{mod}\,m)]+Q_{t-1})\bmod 2^{K-1}=$$

$$=(G_{t-1}[G_{t-1}[x](\mathrm{mod}\,m)]\bmod 2^{K-1}+Q_{t-1}\bmod 2^{K-1})\bmod 2^{K-1}=g_{t-1}[G_{t-1}[x](\mathrm{mod}\,m)]\oplus q_{t-1}.$$

Исследуем правую часть равенства (9):

$$h_{x,q_{t-1}}\varphi_K(G_{t-1})=h_{x,q_{t-1}}\varphi_K\binom{j}{G_{t-1}[j]}_{2^K}^m=h_{x,q_{t-1}}\binom{j}{g_{t-1}[j]}_{2^{K-1}}^m=g_t=\binom{j}{g_t[j]}_{2^{K-1}}^m,$$

где $g_t[j] = g_{t-1}[j], j \neq x$, а $g_t[x] = g_{t-1}[g_{t-1}[x](\mathrm{mod}\, m)] \oplus q_{t-1}$.

Для перехода $j = x$ непосредственно проверяем равенство $s_{t-1}[S_{t-1}[x](\mathrm{mod}\, m)] = s_{t-1}[s_{t-1}[x](\mathrm{mod}\, m)]$.

Равенство (9) доказано. Теорема 1 доказана.

Поиск решения G_1 уравнения $HB_K^{ia}(G_1, x_1, x_2, \ldots, x_L) = y_1 y_2 \ldots y_L$ при известных последовательностях $x_1, x_2, \ldots, x_L$ и $y_1 y_2 \ldots y_L$

Из теоремы 1 следует, что автомат HB_k^{ia} является образом автомата HB_K^{ia} при гомоморфизме $(\psi_k^K, \varphi_k^K, \chi_k^K)$, определенном суперпозицией (последовательным выполнением) гомоморфизмов $(\psi_k, \varphi_k, \chi_k)$, $k \in \{K, K-1, \ldots, k+1\}$. В частности, автомат HB_n^{ia} является образом автомата HB_K^{ia} при гомоморфизме $(\psi_n^K, \varphi_n^K, \chi_n^K)$. Обозначим через $C(HB_k^{ia})$ трудоемкость определения начального состояния $g_1^k \in \Sigma_{2^k}^m$ автомата HB_n^{ia} из уравнения $HB_k^{ia}(g_1^k, x_1 x_2 \ldots x_L) = \chi_k^K(y_1)\chi_k^K(y_2)\ldots\chi_k^K(y_L) = y_1^k y_2^k \ldots y_L^k$ в предположении, что оно единственное.

Поиск решения g_1^{k+1} уравнения

$$HB_{k+1}^{ia}(g_1^k, x_1 x_2 \ldots x_L) = \chi_{k+1}^K(y_1)\chi_{k+1}^K(y_2)\ldots{}_{k+1}^K(y_L) = y_1^{k+1} y_2^{k+1} \ldots y_L^{k+1} \quad (10)$$

для гомоморфного прообраза HB_{k+1}^{ia} автомата HB_k^{ia} при гомоморфизме $(\psi_{k+1}, \varphi_{k+1}, \chi_{k+1})$, $k \in \{K, K-1, \ldots, n+1\}$ автомата HB_{k+1}^{ia} на автомат HB_k^{ia} проведем методом опробования состояний из множества $\varphi_{k+1}^{-1}(g_1^k)$ в автомате A^v.

Будем предполагать, что решение уравнения (10) единственное.

Очевидно, что $|\varphi_{k+1}^{-1}(g_1^k)| = 2, \quad k \in \{n+1, \ldots, K\}$.

Трудоемкость в опробованиях решения уравнения (1) описанным выше методом многоступенчатого гомоморфизма при указанных предположениях равна $C(HB_n^{ia}) + \sum_{k=n+1}^{k=K} |\varphi_{k+1}^{-1}(g_1^k)| = C(HB_n^{ia}) + 2(K-n+1)$.

- Трудоемкость определения ключа для усложненного IA равна $2(K-1) + 2^{2n}$.

Поступила 3 августа 2018 г.

Method of multistatic homomorphism of numbers with feedback on output for an example of equipment IA

A.V. Babash – Dr.Sc.(Phys.-Math.), Professor, HSE (Moscow)
E-mail: avbabash@hse.ru

A cryptanalysis of the complicated version of cipher IA is carried out. The attack of the «multistage homomorphism of the finite automaton» is used. The complexity of the attack is assessed. The complexity of determining the key for a complicated IA is $2(K-1) + 2^{2n}$.

УДК 621.391(075.8)

Организация центра управления событиями информационной безопасности

Е.К. Баранова – доцент, НИУ ВШЭ (Москва)
E-mail: ekbaranova@hse.ru
Е.Д. Завадская – магистрант, НИУ ВШЭ (Москва)
E-mail: ekaterinazav1994@mail.ru

Рассмотрены особенности построения центра управления событиями информационной безопасности (ИБ) SOC (Security Operations Center) в компании и принципы работы системы контроля и выявления инцидентов SIEM (Security Information and Event Management). Приведены шаблоны построения SOC в компании и распространенные ошибки, возникающие при построении и эксплуатации SOC в компаниях.

Ключевые слова: *информационная безопасность, защита информации, управление инцидентами информационной безопасности, SIEM-система, центр управления событиями информационной безопасности, SOC.*

The features of the establishment of Security Operations Center (SOC) in the company and the operation principles of the Security Information and Event Management system (SIEM) are considered; the templates for building SOC in the company are provided; common mistakes that occur during the creation and operation of SOC in the companies are given.

Keywords: *information security, information security management, SIEM-system, Security Operations Center, SOC.*

DOI: 10.18127/j20729472-201804-03

Инцидент информационной безопасности (ИБ) – одно из центральных понятий ИБ в целом. Для обеспечения непрерывности, конфиденциальности и безопасности бизнеса необходимо осуществлять управление инцидентами ИБ. С этой целью в организациях и создаются SOC – центры, осуществляющие обнаружение, мониторинг, реагирование и предотвращение инцидентов ИБ.

Ц е л ь р а б о т ы – рассмотреть особенности организации центра управления событиями ИБ SOC (Security Operations Center) в компании и принципы работы системы контроля и выявления инцидентов SIEM (Security Information and Event Management).

Принципы построения и функционирования SIEM-системы

Центр управления событиями ИБ SOC представляет собой комплекс процессов и программно-аппаратных средств, предназначенных для централизованного сбора и анализа информации о событиях и инцидентах ИБ, поступающих из различных источников ИТ-инфраструктуры, и своевременного реагирования на них.

Мониторинг событий ИБ – процесс постоянного наблюдения за событиями ИБ с целью своевременного выявления действий в информационных системах, которые привели, либо могут привести к реализации угроз ИБ, и реагирования на них [1].

Одним из наиболее популярных решений последних лет для контроля и выявления инцидентов является SIEM-система. Ее популярность, прежде всего, обусловлена значительным объемом задач, которые можно решить с помощью SIEM-системы: сконцентрировать инциденты, фиксируемые другими системами самостоятельно, в рамках единого ядра инцидент-менеджмента; получить удобный инструмент для поиска необходимых событий, разбора инцидентов, хранения собранных данных о событиях и инцидентах ИБ; выявлять статистические отклонения и медленно развивающиеся инциденты за счет анализа больших интервалов и объемов информации с конкретных средств защиты; сопоставлять и коррелировать данные из разных систем и, как следствие, строить сложные цепочки сценариев по обнаружению инцидентов, «обогащать» информацию в логах одних систем данными из других.

Принцип работы SIEM заключается в том, что система собирает информацию, анализирует «на лету» и генерирует предупреждающее сообщение, записывает информацию в базы данных, анализирует поведение на основании предыдущих наблюдений и также генерирует предупреждающее сообщение.

Основной целью построения и функционирования SIEM-систем является значительное повышение уровня ИБ в информационно-телекоммуникационной инфраструктуре за счет обеспечения возможности в режиме, близком к реальному времени, манипулировать информацией о безопасности и осуществлять проактивное (действующее до того, как ситуация станет критической) управление инцидентами и событиями безопасности, которое основывается на автоматических механизмах, использующих информацию о предыстории анализируемых сетевых событий и прогнозе будущих событий, а также на автоматической подстройке параметров мониторинга событий к текущему состоянию защищаемой системы.

Для достижения заявленной цели SIEM-система должна обладать возможностью успешного решения следующего комплекса задач [2]: сбора, обработки и анализа событий безопасности, поступающих в систему из множества гетерогенных источников; обнаружения в режиме реального времени атак и нарушений критериев и политик безопасности; оперативной оценки защищенности информационных, телекоммуникационных и других критически важных ресурсов; анализа и управления рисками ИБ; проведения расследований инцидентов; обнаружения расхождения критически важных ресурсов и бизнес-процессов с внутренними политиками безопасности и приведение их в соответствие друг с другом; принятия эффективных решений по защите информации; формирования отчетных документов.

Обобщенная иерархическая модель SIEM-системы представлена на рис. 1.

Раскроем *содержание основных механизмов функционирования SIEM-системы*.

Нормализация означает приведение форматов записей журналов, собранных из различных источников, к единому внутреннему формату, который затем будет использоваться для их хранения и последующей обработки.

Фильтрация событий безопасности заключается в удалении избыточных событий из поступающих в систему потоков. *Классификация* событий позволяет для атрибутов событий безопасности определить их принадлежность определенным классам. *Агрегация* объединяет события, схожие по определенным признакам. *Корреляция* событий выявляет взаимосвязи между разнородными событиями, что позволяет обнаруживать атаки, а также нарушения критериев и политик безопасности. *Приоритизация* событий определяет значимость и критичность событий безопасности на основании правил, определенных в системе.

Рис. 1. Обобщенная иерархическая модель SIEM-системы

Анализ событий, инцидентов и их последствий включает в себя процедуры моделирования событий, атак и их последствий, анализа уязвимостей и защищенности системы, определения параметров нарушителей, оценки риска, прогнозирования событий и инцидентов. *Генерация отчетов и предупреждений* означает формирование, передачу, отображение и/или печать результатов функционирования. *Принятие решений* определяет выработку мер по реконфигурированию средств защиты с целью предотвращения атак или восстановления безопасности инфраструктуры. *Визуализация* предполагает представление в графическом виде данных, характеризующих результаты анализа событий безопасности и состояние защищаемой системы и ее элементов.

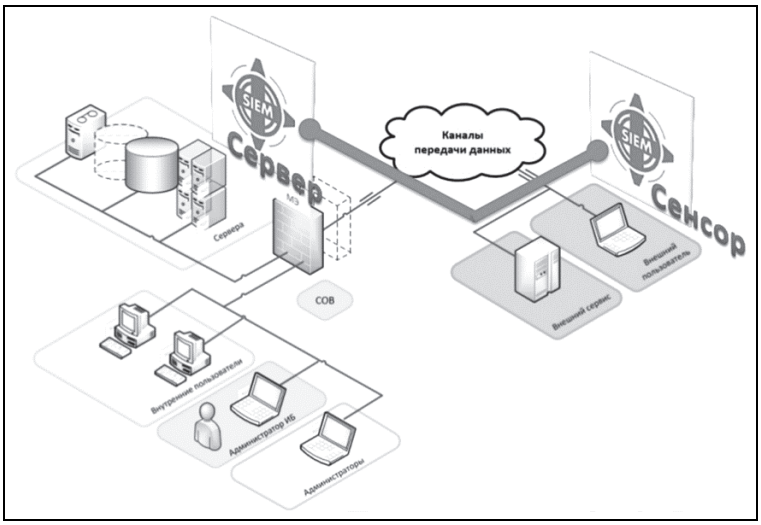

Рис. 2. Пример реализации SIEM-системы

Пример реализации SIEM, представ-

ленный на рис. 2, включает в себя следующие компоненты: агенты (обеспечивают сбор данных из различных источников); серверы-коллекторы (аккумулируют информацию, поступающую от агентов); сервер баз данных (обеспечивает хранение информации); сервер корреляции (анализирует информацию).

SIEM-системы могут использовать для сбора входной информации следующие источники:

системы контроля доступа – применяются для мониторинга контроля доступа к информационным системам и использования привилегий;

DLP-системы (Data Leak Prevention) – поставляют сведения о попытках инсайдерских утечек, нарушении прав доступа;

IDS/IPS-системы (системы обнаружения и предотвращения вторжений) – несут данные о сетевых атаках, изменениях конфигурации и доступа к устройствам;

антивирусные приложения – генерируют события о работоспособности ПО, базах данных, изменении конфигураций и политик, вредоносном коде;

журналы событий серверов и рабочих станций – применяются для контроля доступа, обеспечения непрерывности, соблюдения политик ИБ;

межсетевые экраны – содержат сведения об атаках, вредоносном ПО и прочем;

сетевое активное оборудование – используется для контроля доступа, учета сетевого трафика;

сканеры уязвимостей – предоставляют данные об инвентаризации активов, сервисов, ПО, уязвимостях и топологической структуре;

системы инвентаризации – поставляют данные для контроля активов в инфраструктуре и выявления новых активов;

системы веб-фильтрации – предоставляют данные о посещении сотрудниками подозрительных или запрещенных веб-сайтов.

SIEM-системы способны выявлять: сетевые атаки во внутреннем и внешнем периметрах; вирусные эпидемии или отдельные вирусные заражения; попытки несанкционированного доступа к конфиденциальной информации; мошенничество; ошибки и сбои в работе информационных систем; уязвимости; ошибки конфигураций в средствах защиты и информационных системах; целевые атаки.

В компаниях с развитой ИТ-инфраструктурой и большим числом разнообразных средств защиты без специализированных технических средств выстроить полную картину нарушений в системе ИБ весьма проблематично. Кроме того, внедряемые средства защиты направлены лишь на снижение вероятности возникновения инцидентов ИБ. В случае, если инцидент произошел, без оперативного вмешательства в процесс ликвидации его последствий ущерб может быть весьма серьезным. Поэтому важно своевременно реагировать на выявляемые в ходе мониторинга инциденты.

SOC (Security Operations Center)

Без постоянного мониторинга состояния ИБ, оперативного реагирования на инциденты, управления уязвимостями и контроля выполнения требований законодательства, нормативных актов и внутренних корпоративных политик компаниям довольно сложно быстро и качественно проверять состояние требуемого уровня безопасности, а также поддерживать ИБ на должном уровне.

SIEM-система является ядром любого SOC. Можно выделить несколько предпосылок для создания SOC-центра управления событиями ИБ: постоянно развивающаяся ИТ-инфраструктура; большое число активных средств защиты информации; отсутствие единой картины происходящего в ИТ-инфраструктуре; невозможность оценить эффективность текущих мер защиты информации; невозможность своевременного реагирования на инциденты ИБ; отсутствие сквозного процесса между ИТ, ИБ и бизнесом; необходимость выполнения требований стандартов.

Система управления (мониторинга) событиями ИБ реализует комплексный подход к решению задач сбора, анализа, корреляции и контроля событий ИБ, поступающих от различных средств защиты. На рынке систем управления событиями ИБ представлены технические решения различных производителей. Они отличаются по функционалу, спектру решаемых задач, сфере применения [3, 4].

Базовые компоненты SOC представлены на рис. 3.

SOC – это не только и не столько технические средства, это прежде всего команда, задача которой обнаруживать, анализировать, реагировать, уведомлять о возникновении и предотвращать инциденты ИБ. Чтобы персонал, вооруженный техническими средствами, понимал свои задачи, имел четкие ин-

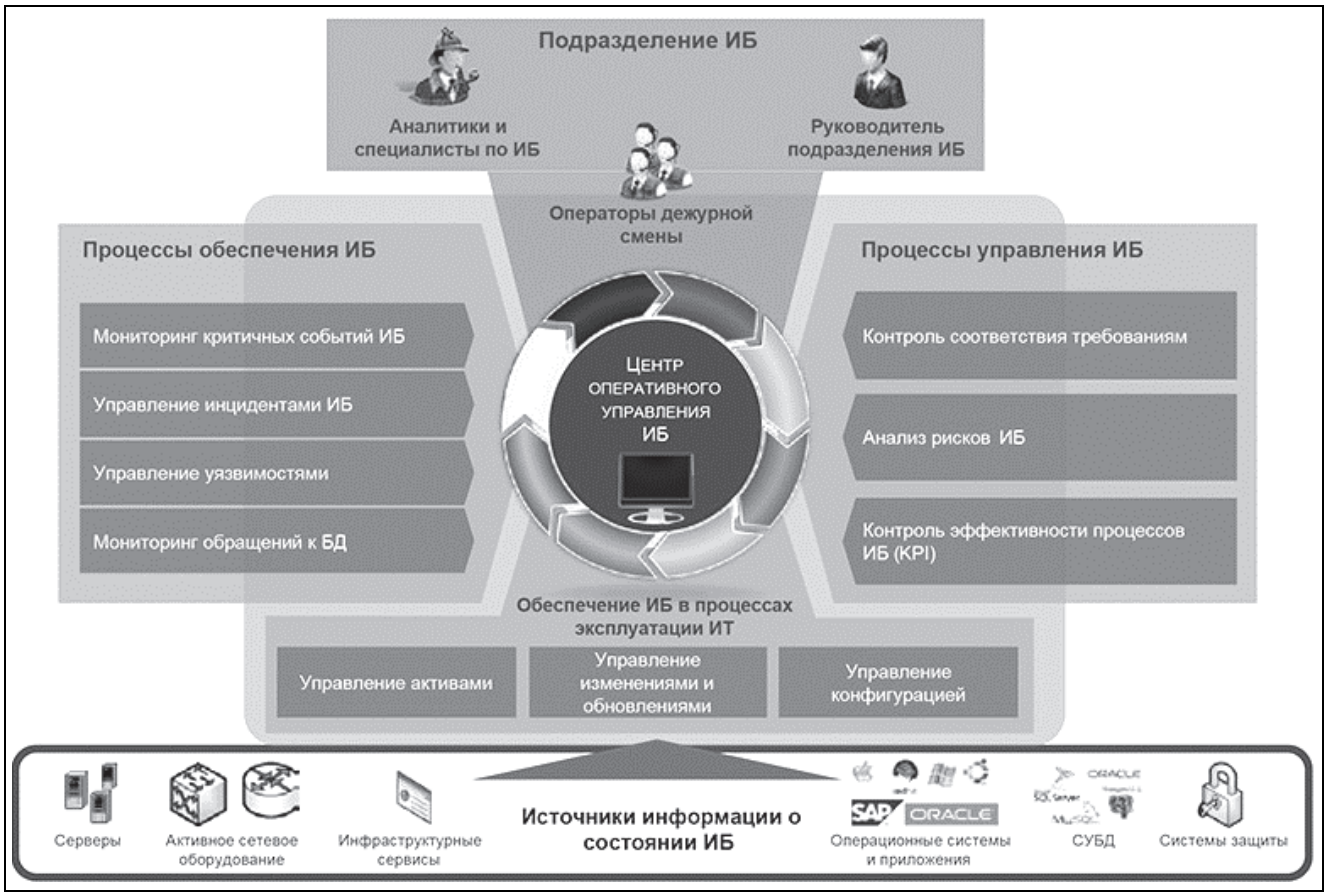

Рис. 3. Базовые компоненты SOC

струкции и KPI (Key Performance Indicators – ключевые показатели эффективности), мог эффективно взаимодействовать внутри SOC и со смежными подразделениями, необходимо выстроить целый ряд процессов в зоне ответственности SOC, направленных на повышение защищенности ИТ-инфраструктуры. Таким образом, формула работающего SOC выглядит так:

SOC = ЛЮДИ + ПРОЦЕССЫ +
+ ТЕХНОЛОГИИ.

Как видно из приведенного определения, SOC это не только люди. Это взаимосвязь процессов, технологий и людей, выполняющих определенные функции. В эффективно функционирующем SOC должны быть реализованы все блоки, приведенные на рис. 4.

Мониторинг является основным процессом SOC. Мониторинг – это систематическое или непрерывное наблюдение за объектом с обеспечением контроля и/или измерения его параметров, а также проведение анализа с целью предсказания изменчивости параметров и принятия решения о необходимости и составе корректирующих и предупреждающих действий [5].

Рис. 4. Составляющие SOC

Структура и порядок функционирования SOC, в первую очередь, определяются целями его создания. Эти цели должны быть определены в соответствии с бизнес-задачами организации и зафиксированы документально. Например, к целям SOC можно отнести: регламентирование и систематизацию деятельности по выявлению и реагированию на инциденты; минимизацию рисков, таких как: несвоевременное обнаружение и оповещение об инциденте, неверная корреляция событий или инцидентов ИБ между собой, выбор недействительных процедур по блокировке распространения инцидента ИБ, утрата свидетельств инцидента и возможности его расследования в будущем; снижение числа инцидентов ИБ и связанных с ними финансовых потерь; снижение совокупных затрат на управление инцидентами ИБ; повышение корпоративной дисциплины.

Эффективность внедрения и использования технических средств максимальна, если компания четко понимает задачи, которые предстоит решать при помощи инструментов SOC.

В работах [6, 7] приводятся несколько шаблонов SOC, которые могут использоваться в организациях (таблица).

Таблица. ***Шаблоны построения SOC***

Виртуальный SOC	
Организационная модель	Внутренний распределенный SOC
Приблизительный размер	1000 пользователей/IP
Видимость	Ограниченная
Полномочия	Полномочия по предупреждению и реагированию на инциденты переданы головной организации
Где возможно использование	Организации малого и среднего бизнеса, муниципалитеты
Малый SOC	
Организационная модель	Внутренний централизованный SOC
Приблизительный размер	10000 пользователей/IP
Видимость	Основные точки периметра, основные хосты
Полномочия	SOC выступает в качестве голосующего при принятии решений, которые стимулируют профилактические или ответные действия
Где возможно использование	Организации среднего бизнеса, университеты, правительственные организации
Большой SOC	
Организационная модель	Внутренний централизованный SOC с элементами распределенного
Приблизительный размер	50000 пользователей/IP
Видимость	Большинство хостов и точек
Полномочия	Самостоятельность при принятии ответных мер, частичные полномочия по предупреждению вторжений
Где возможно использование	Крупные компании и крупные правительственные учреждения
Многоуровневый SOC	
Организационная модель	Внутренний комбинированный распределенный и централизованный, смешанный с координирующим SOC
Приблизительный размер	500000 пользователей/IP
Видимость	Данные напрямую поступают от различных источников, большинство данных передается в соподчиненные SOC
Полномочия	Самостоятельность при принятии ответных мер, которые, в свою очередь, оказывают влияние на соподчиненные SOC, частичные полномочия по предупреждению вторжений
Где возможно использование	Международные конгломераты, мультидисциплинарные правительственные организации
Национальный SOC	
Организационная модель	Координирующий SOC
Приблизительный размер	50000000 пользователей/IP
Видимость	Ограниченный, но распространенный доступ к данным, зависит от настроек
Полномочия	Консультационный характер
Где возможно использование	SOC, обслуживающие целые правительства и страны

Среди самых распространенных ошибок при построении и эксплуатации SOC в организациях можно выделить следующие: недостаточная поддержка руководства; плохо сформулированная и плохо определенная цель; низкая квалификация специалистов, работающих со сложными технологиями, поскольку многие организации выделяют достаточно большую долю бюджета на технические решения, забывая при этом об уровне знаний и компетенций своих специалистов; решение специалистами по ИБ второстепенных задач (переустановить ПО, купить ПК и др.), которое приводит к тому, что задачи, имеющие более высокий приоритет, будут решены не вовремя; работа лишь для того, чтобы соответствовать требованиям регуляторов, а не для того, чтобы повысить уровень безопасности в организации.

- При помощи SOC становится возможным организовать процесс непрерывного совершенствования защитных мер для обеспечения безопасности. Постоянный анализ текущих событий и инцидентов ИБ, выяснение причин их возникновения с привлечением различных подразделений позволяет оценить эффективность текущих мер защиты, понять их недостатки и выработать предложения по их замене или корректировке.

  Внедрение SOC позволяет снизить прямые и косвенные затраты. При небольшом штате сотрудников, когда «не хватает рук», SOC позволяет сократить ресурсы, необходимые для ручной обработки событий ИБ при увеличении числа контролируемых средств защиты. При этом SOC не требует увеличения штата, а, напротив, позволяет оптимизировать работу сотрудников путем сведения данных на одну консоль и автоматизации проводимого анализа событий ИБ.

  Средствами центра управления событиями ИБ можно разделить полномочия контроля за ИТ-системами. Средства защиты, их администрирование и эксплуатация, как правило, находятся в ведении подразделения ИТ, в то время как подразделениям ИБ отводятся только функции контроля. SOC – это, пожалуй, единственный инструмент контроля в руках у подразделений ИБ, позволяющий им отслеживать действия в ИТ-системах, что объективно снижает влияние человеческого фактора и повышает уровень ИБ компании.

  Данные, предоставляемые SOC, существенно уточняют оценку рисков, которая является основой в выборе тех или иных мер защиты. Кроме того, формализация процедур снижает косвенные затраты компании, так как вопросы согласований без качественного обоснования занимают значительное количество рабочего времени сотрудников.

  Внедрение и системное использование системы менеджмента ИБ позволяет уменьшить негативное воздействие инцидентов ИБ на бизнес, усилить акцент на их предупреждение, улучшить качество результатов оценки и управления рисками ИБ, что в итоге позволяет повысить общий уровень ИБ компании.

  Помимо повышения защиты бизнеса, построение процесса управления инцидентами зачастую преследует цель соответствия требованиям различных отраслевых и международных стандартов, большинство из которых содержат требования, касающиеся непосредственно не только мониторинга обращений к критичным данным, но и процедуры работы с инцидентами ИБ.

Литература

1. Организация Security Operation Center (SOC). ЗАО НИП «Информзащита». URL = http://docplayer.ru/46349479-Organizaciya-security-operation-center-soc.html. (Дата обращения: 8.06.2018).
2. *Котенко И.В.*, *Саенко И.Б.*, *Полубелова О.В.*, *Чечулин А.А.* Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды Санкт-Петербургского института информатики и автоматизации РАН (СПИИРАН). СПб.: 2012. № 20. С. 27−56.
3. *Медведев Артем* Самый безопасный SOC // Jet Info. № 3. URL = http://www.jetinfo.ru/stati/samyj-bezopasnyj-soc. (Дата обращения: 18.05.2018).
4. *Бабаш А.В.*, *Баранова Е.К.* Актуальные вопросы защиты информации: монография. М.: ИНФРА-М. РИОР. 2017.
5. *Бабаш А.В.*, *Баранова Е.К.* Особенности управления инцидентами информационной безопасности // Сб. научных работ XVI научно-практич. конф. «Современные информационные технологии в управлении и образовании». М.: ФБГУ НИИ «Восход». 2017. С. 81−94.
6. *Федорченко А.В.*, *Левшун Д.С.*, *Чечулин А.А.*, *Котенко И.В.* Анализ методов корреляции событий безопасности в SIEM-системах // Труды Санкт-Петербургского института информатики и автоматизации РАН (СПИИРАН). СПб.: 2016. № 4(47). URL = www.proceedings.spiiras.nw.ru.
7. *Carson Zimmerman* Ten Strategies of a World-Class Cybersecurity Operations Center. MITRE. 2014. URL = www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf. (Дата обращения: 8.06.2018).

Поступила 3 августа 2018 г.

The establishment of security operations center

E.K. Baranova – Associate Professor, HSE (Moscow)
E-mail: ekbaranova@hse.ru
E.D. Zavadskaya – Undergraduate, HSE (Moscow)
E-mail: ekaterinazav1994@mail.ru

The features of the establishment of Security Operations Center (SOC) in the company and the operation principles of the Security Information and Event Management system (SIEM) are considered; the templates for building SOC in the company are provided; common mistakes that occur during the creation and operation of SOC in the companies are given. The introduction and systematic use of the IS management system allows to reduce the negative impact of IS incidents on the business, increase the emphasis on their prevention, improve the quality of the results of the assessment and management of IS risks, which ultimately allows to increase the company's overall IS level.

References

1. Organizaciya Security Operation Center (SOC). ZAO NIP «Iformzashitaa». URL = http://docplayer.ru/46349479-Organizaciya-security-operation-center-soc.html. (Visited on: 8.06.2018).
2. *Kotenko I.V., Saenko I.B., Polubelova O.V., Chechulin A.A.* Primenenie tekhnologii upravleniya informaciey i sobitiyami bezopasnosti dlya zashiti informacii v kriticheski vagnikh infractrukturakh // Trudi Sankt-Peterburgskogo instituta informatiki i avtovatizacii RAN (SPIIRAN). SPb.: 2012. № 20. S. 27–56.
3. *Medvedev Artem* Samiy bezopasniy OS // Jet Info. № 3. URL = http://www.jetinfo.ru/stati/samyj-bezopasnyj-soc. (Visited on: 18.05.2018).
4. *Babash A.V., Baranova E.K.* Aktualnie voprosi zashiti informacii: monografiya. M.: INFRA-M. RIOP. 2017.
5. *Babash A.V., Baranova E.K.* Osobennosti upravleniya inzidentami informacionnoy bezopasnosti // Sb. nauchnikh rabot XVI nauchno-praktich. konf. «Sovremennie informacionnie tekhnologii v upravlenii I obrazovanii». M.: FBGU NII «Voskhod». 2017. S. 81–94.
6. *Fedorchenko A.B., Levshun D.S., Chechulin A.A., Kotenko I.V.* Analiz metodov korrelyaii sobitiy bezopasnosti v SIEM-sistemakh // Trudi Sankt-Peterburgskogo instituta informatiki I avtovatizacii RAN (SPIIRAN). SPb.: 2016. № 4(47). URL = www.proceedings.spiiras.nw.ru.
7. *Carson Zimmerman* Ten Strategies of a World-Class Cybersecurity Operations Center. MITRE. 2014. URL = www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf. (Visited on: 8.06.2018).

УДК 004.8

Анализ личностных черт пользователей социальных сетей на основе автоматической обработки их профилей[1]

М.А. Станкевич – инженер, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: stankevich@isa.ru
И.В. Смирнов – к.ф.-м.н., зав. отделом, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: ivs@isa.ru
Н.А. Игнатьев – студент, РУДН (Москва)
E-mail: naignatiev@yandex.com
Н.В. Кисельникова – к.псих.н., зав. лабораторией,
Психологический институт Российской академии образования (Москва)
E-mail: nv.pirao@gmail.com
М.М. Данина – к.псих.н., ст. науч. сотрудник,
Психологический институт Российской академии образования (Москва)
E-mail: mdanina@yandex.ru

Проведен анализ модели Большой Пятерки личностных черт пользователей социальной сетей при помощи автоматической обработки данных их персональных профилей. На основе полученного набора данных была произведена мульти-классовая классификация, целью которой было автоматическое определение уровня выраженности каждой из пяти личностных черт пользователей.

Ключевые слова: *Большая Пятерка личностных черт, анализ социальных сетей, машинное обучение, классификация.*

This work is devoted to the analysis of the Big Five personality model of users in social media by automatic processing of their social media profiles. On the basis of the obtained data set, a multi-class classification was made, the purpose of which was to automatically determine the level of expression of each of the five personal traits of users.

Keywords: *Big Five personality traits, social media analysis, machine learning, classification.*

DOI: 10.18127/j20729472-201804-04

Большая Пятерка личностных черт – это модель представления черт человека, которая описывает личность при помощи следующих пяти черт: невротизм, экстраверсия, готовность к согласию, открытость опыту и сознательность [1]. В общепринятой практике уровень этих черт определяется при помощи стандартизированных опросников и методик, результаты обработки которых можно представить в виде значения на численной шкале, характеризующей выраженность той или иной личностной черты. Возросшая популярность социальных сетей позволяет изучать различные психологические характеристики их пользователей при помощи автоматического анализа данных профилей этих пользователей и алгоритмов машинного обучения. На данный момент можно выделить ряд работ, посвященных анализу и предсказыванию пяти личностных черт среди пользователей англоязычных социальных сетей [2, 3]. Однако аналогичная проблема для русскоязычных социальных сетей практически не рассмотрена.

Существует направление исследований, в котором рассматривается использование данных социальных сетей в качестве материала для анализа и предсказания различных психологических характеристик их пользователей. Одна из самых широко рассмотренных проблем – это обнаружение депрессии у пользователей социальных сетей. Например, открытый проект CLPsych 2015 предлагал своим участникам представить свои классификационные модели, способные установить наличие депрессии у пользователя на основе обработки коллекции его текстовых сообщений [5]. Это исследование, как и ряд других схожих работ [6, 7], в основном базируется на обработке текстовых сообщениях пользователей, где в качестве основных признаков выступают данные об использованной лексике. Однако можно выделить работы [8, 9], где в качестве признаков использовалась информация об активности пользователя в социальной сети: число подписчиков, друзей, сообщений и др.

Одно из самых крупных исследований, посвященных анализу Большой Пятерки личностных черт

[1] Работа выполнена при поддержке РФФИ, проект № 17-29-02225 «офи_м».

пользователей социальных сетей [10], основывается на данных 75 000 испытуемых из Facebook, прошедших стандартизированный опросник и предоставивших доступ к своим текстовым сообщениям. В ходе работы был проведен корреляционный анализ и была выявлена лексика пользователей, которая имеет наиболее значимые корреляции с уровнем выраженности пяти их личностных черт. Представленные результаты показали, что существуют явные зависимости между используемой пользователями лексикой в социальной сети и личностными чертами этих людей.

В другой работе [11], основанной на наборе данных текстовых сообщений 279 пользователей Twitter, рассматривается задача построения регрессионной модели, способной предсказывать личностные черты пользователей. Авторы работы представляли исходные значения личностных черт (баллы), полученные из результатов опросников, в виде значения на нормализованной шкале от 0 до 1. Далее использовался популярный инструмент LIWC (Linguistic Inquiry and Word Count) [12] для выделения порядка 80 признаков из текста пользователей. Кроме того, применялись данные из MRC Psycholinguistic Database [13] для составления лексических признаков и признаков активности пользователей в социальной сети. По результатам регрессионного анализа авторам удалось достичь приблизительно 15% средней абсолютной ошибки для каждой из личностных черт. Спорным можно считать решение авторов использовать для оценки точности среднюю абсолютную ошибку вместо среднеквадратичного отклонения, стандартного для задачи регрессионного анализа.

Таким образом, изучив научные работы по данной теме, можно сделать следующие выводы. Во-первых, текстовую информацию, а именно сообщения пользователей в социальных сетях, можно использовать для составления эффективных признаков для анализа Большой Пятерки личностных черт и других психологических характеристик. Во-вторых, рассмотренная проблема достаточно хорошо изучена для английского языка и англоязычных социальных сетей, но для русскоязычного сегмента подобные исследования отсутствуют. Именно поэтому было принято решение рассмотреть данную проблематику.

Цель работы – описать методы анализа Большой Пятерки личностных черт пользователей ВКонтакте при помощи автоматической обработки их данных в социальной сети и рассмотреть модели машинного обучения, которые способны выявить уровень личностных черт этих пользователей. В свою очередь, чтобы провести подобное исследование, также потребовалось составить собственный набор данных.

Метод выявления личностных черт пользователей социальных сетей

Чтобы сформировать набор данных, использовалось встроенное приложение ВКонтакте. В данном приложении пользователям социальной сети предлагалось пройти стандартизированную методику NEO-FFI, результаты которой можно интерпретировать в виде целого значения на шкале от 0 до 48 для каждой личностной черты. Данные значения отражают степень выраженности невротизма, экстраверсии, готовности к согласию, открытости опыту и сознательности испытуемого. Также запрашивалось разрешение на обработку данных персональных страниц у испытуемых. Таким образом, удалось собрать информацию об активности 165 пользователей, полученную при помощи API ВКонтакте.

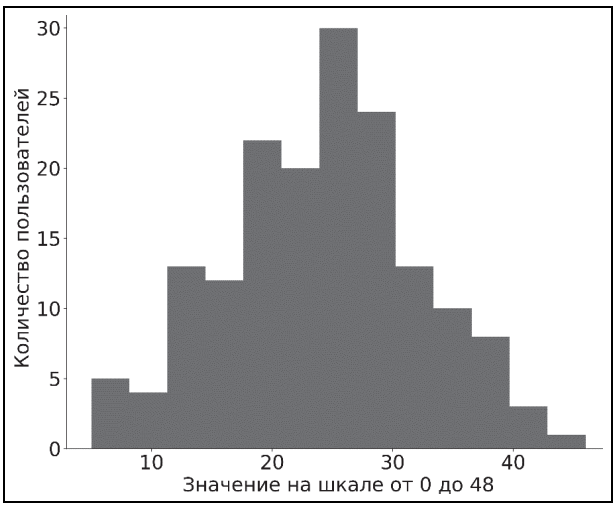

Рис. 1. Гистограмма значений невротизма среди пользователей из набора данных

Собранные данные можно разделить на две части. Первая содержит общую информацию о пользователях: число друзей, число подписчиков, пол, число групп и информация о стандартных вопросах ВКонтакте. Вторая часть содержит все сообщения пользователей на их персональных страницах, выложенные в период с 1 января 2017 г. по февраль 2018 г.

Обработав данные о результатах прохождения опросников, можно сделать вывод, что большинство пользователей имеют средние значения личностных черт по каждой из шкал. На рис. 1 продемонстрирована гистограмма значения невротизма среди испытуемых из набора данных.

В данной работе было принято решение разделить исходную шкалу от 0 до 48 баллов на три интервала. Каждая из личностных черт Большой Пятерки пользователя была представлена в виде следующих классов: низкий уровень (0−20), средний уровень (21−32) и высокий уровень (33−48). Данный подход позволяет свести поставленную задачу к мульти-классовой классификации. Таким образом, от модели машинного обучения потребуется установить низкий, средний или высокий уровень той или иной личностной черты для пользователя. Итоговая статистика по Большой Пятерке личностных черт среди 165 пользователей представлена в табл. 1. Изучив данные из табл. 1, можно сделать вывод, что средний уровень преобладает во всех личностных чертах, хотя он покрывает самый короткий интервал исходных баллов.

Таблица 1. ***Статистика по Большой Пятерке личностных черт среди пользователей из выборки (% от общего числа пользователей)***

Невротизм	Низкий уровень	33,9
	Средний уровень	49,6
	Высокий уровень	16,3
Сознательность	Низкий уровень	19,3
	Средний уровень	55,7
	Высокий уровень	24,8
Экстраверсия	Низкий уровень	27,8
	Средний уровень	58,1
	Высокий уровень	13,9
Открытость опыту	Низкий уровень	10,6
	Средний уровень	66,3
	Высокий уровень	23,1
Готовность к согласию	Низкий уровень	15,1
	Средний уровень	73,3
	Высокий уровень	11,5

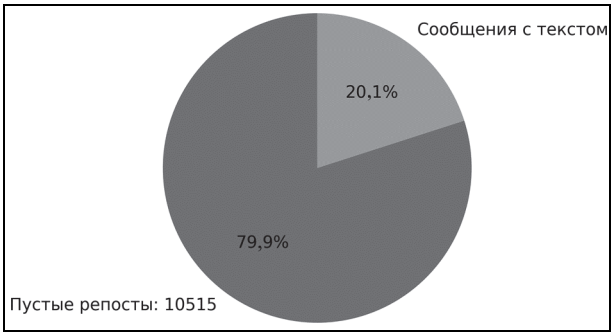

Рис. 2. Диаграмма соотношения пустых репостов и сообщений с текстом

В качестве общих признаков были использованы: число друзей, число подписчиков, число сообществ, число фотографий и аудиозаписей, пол. Формат персональных страниц ВКонтакте содержит достаточно много информации о пользователе, которая представляется в виде ответов на стандартные вопросы, предлагаемые пользователю. Наличие или отсутствие ответов на эти вопросы было представлено в виде бинарных признаков. Было сделано предположение, что подобные признаки могут в целом отражать готовность пользователя делиться информацией о себе с другими людьми, что может быть значимым в задаче выявления личностных черт. Число лайков, комментариев и репостов, оставленных на публичных сообщениях пользователей, было представлено в виде средних значений относительно общего числа сообщений. Так как для всех пользователей информация собиралась за идентичный период времени, также было использовано общее число сообщений каждого пользователя в виде признака. Временные отметки на сообщениях были применены для расчета числа сообщений, которые были отправлены в ночное время суток (00:00…06:00).

Изучив сообщения пользователей, авторы пришли к выводу, что они содержат крайне ограниченное количество текстовой информации. Большинство сообщений пользователей в ВКонтакте – репосты, представляющие из себя сообщения, которые были написаны другими людьми или сообществами. Пользователи могут сделать репост этой записи к себе на страницу, но также могут не добавлять к нему никакого собственного комментария. Таким образом, подавляющее число собранных сообщений являются пустыми репостами (рис. 2). Данный факт заставил отказаться от использования текстовых признаков при текущем размере набора данных. Тем не менее, были добавлены следующие признаки: общее число слов и предложений, число многоточий и доля верхнего регистра в тексте.

Результаты экспериментов

После этапа составления пространства признаков были подготовлены классификационные модели, основанные на Sci-kit Learn [14] мульти-классовых реализациях алгоритма случайного леса и метода опорных векторов. Результаты классификации представлены в табл. 2. Полученные результаты являются результатом усреднения десяти прогонов четырехкратного скользящего контроля по всей выборке из 165 испытуемых.

Таблица 2. ***Результаты классификации***

Big Five trait	Recall, %	Precision, %	F1-score, %
Random Forest			
Neuroticism	49,07	53,01	49,51
Conscientiousness	35,19	37,12	35,46
Extraversion	46,41	46,79	46,38
Openness to experience	44,65	47,50	45,46
Agreeableness	51,15	56,04	53,15
SVM			
Neuroticism	33,88	49,17	33,38
Conscientiousness	37,54	41,69	36,17
Extraversion	40,02	47,04	41,78
Openness to experience	32,28	52,47	35,07
Agreeableness	38,10	57,59	43,26

Наилучшие результаты в экспериментах были показаны для готовности к согласию и невротизма – 51% и 49% F1-меры соответственно. Самая низкая точность была показана с уровнем сознательности – 36% F1-меры. В целом, алгоритм случайного леса значительно лучше справился с задачей мульти-классовой классификации.

Нельзя назвать полученные результаты высокими. Связано это с тем, что на текущем этапе пришлось отказаться от лексических признаков, которые, в свою очередь, показывали свою эффективность в похожих исследованиях, основанных на англоязычных социальных сетях.

- Проведен анализ Большой Пятерки личностных черт пользователей ВКонтакте при помощи автоматической обработки их профилей. С использованием выделенных из исходного набора данных признаков осуществлена мульти-классовая классификация с целью определения уровня выраженности невротизма, экстраверсии, готовности к согласию, открытости опыту и сознательности пользователей ВКонтакте.

  На текущем этапе экспериментов не удалось показать очень высокие результаты. Чтобы повысить точность классификации, потребуется значительно большая выборка. Более того, ограниченность набора данных делает невозможным использование лексических признаков на данном этапе. Таким образом, основным направлением последующих работ является расширение набора данных, что позволит расширить пространство используемых признаков и получить значительно более высокую точность.

Литература

1. *Gosling S.D.*, *Rentfrow P.J.*, Swann *Jr W.B.* A very brief measure of the Big-Five personality domains // Journal of Research in personality. 2003. Т. 37. № 6. С. 504−528.
2. *Ortigosa A.*, *Carro R.M.*, *Quiroga J.I.* Predicting user personality by mining social interactions in Facebook // Journal of computer and System Sciences. 2014. Т. 80. № 1. С. 57−71.
3. *Schwartz H.A. et al*. Personality, gender, and age in the language of social media: The open-vocabulary approach // PloS one. 2013. Т. 8. № 9. С. e73791.
4. *Costa P.T.*, *McCrae R.R.* NEO five-factor inventory (NEO-FFI). Odessa, FL: Psychological Assessment Resources. 1989.
5. *Coppersmith G. et al*. CLPsych 2015 shared task: Depression and PTSD on Twitter // Proc. of the 2nd Workshop on Computational Linguistics and Clinical Psychology: From Linguistic Signal to Clinical Reality. 2015. С. 31−39.
6. *Yazdavar A.H. et al*. Semi-supervised approach to monitoring clinical depressive symptoms in social media // Proc. of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. ACM. 2017. С. 1191−1198.
7. *Jamil Z.* Monitoring Tweets for Depression to Detect At-risk Users: дис. Université d'Ottawa/University of Ottawa. 2017.
8. *De Choudhury M.*, *Counts S.*, *Horvitz E.* Social media as a measurement tool of depression in populations // Proc. of the 5th Annual ACM Web Science Conference. ACM. 2013. С. 47−56.
9. *Wang X. et al*. A depression detection model based on sentiment analysis in micro-blog social network // Pacific-Asia Conference on Knowledge Discovery and Data Mining. Springer, Berlin, Heidelberg. 2013. С. 201−213.
10. *Cobb-Clark D.A.*, *Schurer S.* The stability of big-five personality traits // Economics Letters. 2012. Т. 115. № 1. С. 11−15.
11. *Golbeck J. et al*. Predicting personality from twitter // Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Inernational Conference on Social Computing (SocialCom). 2011. С. 149−156.
12. *Pennebaker J.W.*, *Francis M.E.*, *Booth R.J.* Linguistic inquiry and word count: LIWC 2001 // Mahway: Lawrence Erlbaum Associates. 2001. Т. 71.
13. *Coltheart M.* The MRC psycholinguistic database // The Quarterly Journal of Experimental Psychology. 1981. Т. 33. № 4. С. 497−505.
14. *Pedregosa F. et al*. Scikit-learn: Machine learning in Python // Journal of machine learning research. Oct. 2011. Т. 12. С. 2825−2830.

Поступила 3 августа 2018 г.

Analysis of personality traits of social media users by automatic profile processing

M.A. Stankevich – Engineer, FRC «Computer Science and Control» of RAS (Moscow)
E-mail: stankevich@isa.ru
I.V. Smirnov – Ph.D.(Phys.-Math.), Head of Department, FRC «Computer Science and Control» of RAS (Moscow)
E-mail: ivs@isa.ru
N.A. Ignatiev – Student, RUDN Univercity (Moscow)
E-mail: naignatiev@yandex.com
N.V. Kiselnikova – Ph.D.(Psych.), Head of Laboratory, Psychological Institute of Russian Academy of Education (Moscow)
E-mail: nv.pirao@gmail.com
M.M. Danina – Ph.D.(Psych.), Senior Research Scientist, Psychological Institute of Russian Academy of Education (Moscow)
E-mail: mdanina@yandex.ru

This work is devoted to the analysis of the Big Five personality model of users in social media by automatic processing of their social media profiles. To form the dataset, we asked VKontakte users to complete NEO-FFI questionnaire in order to reveal their level of neuroticism, extraversion, agreeableness, openness to experience, and conscientiousness. Then, we utilized the data from the personal pages of 165 users who granted permission to process their data to form the features and perform a multiclass classification task. On the basis of the obtained data set, a multi-class classification was made, the purpose of which was to automatically determine the level of expression of each of the five personal traits of users.

References

1. *Gosling S.D.*, *Rentfrow P.J.*, Swann *Jr W.B.* A very brief measure of the Big-Five personality domains // Journal of Research in personality. 2003. T. 37. № 6. S. 504–528.
2. *Ortigosa A.*, *Carro R.M.*, *Quiroga J.I.* Predicting user personality by mining social interactions in Facebook // Journal of computer and System Sciences. 2014. T. 80. № 1. S. 57–71.
3. *Schwartz H.A. et al*. Personality, gender, and age in the language of social media: The open-vocabulary approach // PloS one. 2013. T. 8. № 9. S. e73791.
4. *Costa P.T.*, *McCrae R.R.* NEO five-factor inventory (NEO-FFI). Odessa, FL: Psychological Assessment Resources. 1989.
5. *Coppersmith G. et al*. CLPsych 2015 shared task: Depression and PTSD on Twitter // Proc. of the 2nd Workshop on Computational Linguistics and Clinical Psychology: From Linguistic Signal to Clinical Reality. 2015. S. 31–39.
6. *Yazdavar A.H. et al*. Semi-supervised approach to monitoring clinical depressive symptoms in social media // Proc. of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. ACM. 2017. S. 1191–1198.
7. *Jamil Z.* Monitoring Tweets for Depression to Detect At-risk Users: dis. Université d'Ottawa/University of Ottawa. 2017.
8. *De Choudhury M.*, *Counts S.*, *Horvitz E.* Social media as a measurement tool of depression in populations // Proc. of the 5th Annual ACM Web Science Conference. ACM. 2013. S. 47–56.
9. *Wang X. et al*. A depression detection model based on sentiment analysis in micro-blog social network // Pacific-Asia Conference on Knowledge Discovery and Data Mining. Springer, Berlin, Heidelberg. 2013. S. 201–213.
10. *Cobb-Clark D.A.*, *Schurer S.* The stability of big-five personality traits // Economics Letters. 2012. T. 115. № 1. S. 11–15.
11. *Golbeck J. et al*. Predicting personality from twitter // Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Inernational Conference on Social Computing (SocialCom). 2011. S. 149–156.
12. *Pennebaker J.W.*, *Francis M.E.*, *Booth R.J.* Linguistic inquiry and word count: LIWC 2001 // Mahway: Lawrence Erlbaum Associates. 2001. T. 71.
13. *Coltheart M.* The MRC psycholinguistic database // The Quarterly Journal of Experimental Psychology. 1981. T. 33. № 4. S. 497–505.
14. *Pedregosa F. et al*. Scikit-learn: Machine learning in Python // Journal of machine learning research. Oct. 2011. T. 12. S. 2825–2830.

УДК 004

Применение алгоритмов машинного обучения при решении задач информационной безопасности

Ю.В. Виноградов – начальник отдела, ООО «ЦСС-Сервис» (Москва)
E-mail: vinogradov_yv@ssec.ru
А.Н. Назаров – д.т.н., профессор, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: a.nazarov06@bk.ru
А.К. Сычев – вед. инженер-математик, ООО «ЦСС-Сервис» (Москва)
E-mail: sychev_a_k@mail.ru

Изучен вопрос использования алгоритмов машинного обучения при решении задач информационной безопасности, а именно: при построении систем обнаружения вторжений (IDS) нового поколения. Рассмотрены основные недостатки традиционных IDS (основанных на сигнатурных правилах) и предложены методы их решения с помощью применения алгоритмов машинного обучения. Приведены новые методы применения алгоритмов машинного обучения, с помощью которых можно детектировать как уже известные угрозы, так и ранее не замеченные вариации известных угроз.

Ключевые слова: *мониторинг, системы обнаружения вторжений, выявление аномалий, сетевой трафик, машинное обучение, глубинные нейронные сети.*

The article studies the use of machine learning algorithms in solving information security problems, namely, in the construction of next-generation intrusion detection systems (IDS). The main drawbacks of traditional IDS (based on signature rules) are considered and methods for their solution are proposed using the algorithms of machine learning. The article presents new methods of applying machine learning algorithms, with the help of which it is possible to detect both already known threats and previously not seen variations of known threats.

Keywords: *monitoring, IDS, anomaly detection, network traffic, machine learning, deep neural networks.*

DOI: 10.18127/j20729472-201804-05

Киберугрозы представляют собой постоянную опасность для мировой экономики и, по прогнозам, ущербы от киберпреступлений вырастут на 6 трлн долларов в год к 2021 г. В результате индустрия кибербезопасности вкладывает значительные средства в машинное обучение в надежде достичь динамичного сдерживания роста угроз [1].

Все больше предприятий начинают изучать возможности использования машинного обучения, чтобы решить проблему сложного мониторинга, которую создает шифрование, и уменьшить время действия злоумышленников. Благодаря усовершенствованным возможностям машинного обучения можно укрепить оборону сети и со временем «обучить» системы безопасности автоматически выявлять нехарактерные модели поведения субъектов и информационных потоков (сетевого трафика), которые могут свидетельствовать о вредоносной активности [2].

Цель работы – изучить вопрос использования алгоритмов машинного обучения при решении задач информационной безопасности, а именно: при построении систем обнаружения вторжений (IDS) нового поколения.

Традиционные решения для обнаружения вторжений и вредоносных программ основаны на известных сигнатурах и шаблонах для обнаружения угроз. Они сталкиваются с проблемой обнаружения новых и никогда ранее невидимых атак. Традиционные подходы, основанные на правилах и сигнатурах, будут представлять собой лишь одну часть гораздо более широкой стратегии безопасности, которая включает в себя методы обнаружения и потенциально автоматические процессы реагирования и восстановления инцидентов.

Современные вредоносные программы характеризуются следующими признаками, которые традиционные IDS обнаружить не могут:

1. Вредоносные программы часто используют уязвимости нулевого дня для компрометации цели. Традиционные IDS выявить данные типы атак не могут из-за отсутствия сигнатур;

2. Взаимодействие вредоносной программы с управляющим сервером зачастую осуществляется с использованием шифрованных туннелей (SSL), что делает традиционные IDS неспособными проверить их содержимое;

3. Вредоносные программы обычно скрываются в сети в течение длительного времени и работают в скрытом режиме (например, могут выходить на связь с управляющим сервером раз в месяц). Традиционные IDS, которые не обладают способностью сохранять и коррелировать события из разных источников в течение длительного времени, неспособны обнаружить такую вредоносную активность.

Приведенные недостатки традиционных IDS могут решить системы, основанные на алгоритмах машинного обучения. Системы обнаружения атак нового поколения (построенные с использованием алгоритмов машинного обучения) могут решать следующие з а д а ч и :

1. Построение модели корпоративной сети, составление ее профиля (используемые порты и протоколы, ресурсы и приложения; география подключений; длительность сессий и др.). Используется для алгоритмов машинного обучения с целью поиска аномального отклонения текущего состояния сети от ее нормального профиля. Например, решение задачи выявления вредоносного зашифрованного трафика (п.6).

2. Поиск аномалий (атак, в том числе неизвестных ранее) внутри корпоративной сети. Обнаружение аномалий – это технология обнаружения вредоносного поведения путем сравнения текущих действий с узнаваемыми «нормальными» профилями действий и сущностей, которые могут быть учетными записями пользователей, хостами, сетями или приложениями.

Алгоритмы обнаружения аномалий можно разделить на следующие п о д г р у п п ы :

Статистические алгоритмы выявления аномалий. В [3] предлагается новая система обнаружения вторжений, которая выполняет обнаружение аномалий, изучая изменение в энтропии, связанной с сетевым трафиком. С этой целью трафик сначала агрегируется с помощью случайных структур данных (трехмерных обратимых эскизов), а затем энтропия разных показателей сетевого трафика вычисляется с использованием нескольких определений энтропии (энтропия Шеннона, энтропия Цаллиса, энтропия Реньи, расхождение Кульбака–Лейблера, расхождение Дженсена–Шеннона) для обнаружения аномального поведения.

Алгоритмы выявления аномалий на основе кластерного анализа, а также улучшение данных алгоритмов путем комбинации их с алгоритмами обучения с учителем. В [4] авторы применяют алгоритм обучения с частичным привлечением учителя для выявления DDoS-атак. Разработанный авторами метод основан на оценке энтропии, приросте информации, бикластеризации и чрезвычайно рандомизированных деревьев.

Алгоритмы выявления аномалий на основе глубинных нейронных сетей. Эти алгоритмы включают в себя д в а э т а п а .

Э т а п 1 . Нейронная сеть обучается распознаванию классов нормального поведения на обучающей выборке. Одной из больших проблем построения систем обнаружения нового поколения является отсутствие достаточного количества размеченного набора данных для обучения алгоритмов классификации.

Э т а п 2 . Каждый экземпляр поступает в качестве входного сигнала нейронной сети. Система, основанная на нейронных сетях, может распознавать как один, так и несколько классов нормального поведения.

В последнее время широкое распространение получила технология глубинных нейронных сетей для решения задач выявления аномалий. Также глубинные нейронные сети используются для выбора признаков сетевого трафика, которые в дальнейшем будут использоваться алгоритмами классификации. В [5] представлены методики применения глубинных нейронных сетей, рекуррентных нейронных сетей, ограниченных машин Больцмана и глубоких сетей убеждений для обнаружения аномалий в сетевом трафике.

3. Обогащение данных. Поскольку большая платформа данных обладает множеством различных видов данных из огромного числа источников, очень важно использовать гетерогенные данные для обогащения друг друга, чтобы обеспечить дополнительные контексты. Цель таких обогащений состоит в том, чтобы автоматически загружать данные, относящиеся к безопасности, и чтобы аналитикам не требовалось вручную проверять эти источники данных. Приведем примеры обогащений данных безопасности: обогащение внутренних данных корпоративной сети с помощью информации о внешних угрозах (Threat Intelligence); обогащение логов пользователей прокси-сервера с метаданными электронных писем, в теле которых присутствуют ссылки на внешние ресурсы и др.

4. Выявление взаимосвязанных событий в большом объеме данных. С помощью аналитики больших данных сотрудники безопасности могут анализировать целый ряд новых наборов данных за длительный период времени, что дает им больше информации о том, что происходит в их сети. Это позволит при выявлении атаки оперативно определить, на какой стадии «Kill Chain» [6] она находится и, впоследствии, за счет большого количества исходных данных найти начало атаки и IP-адрес злоумышленника.

5. Прогнозирование сбоев и атак в корпоративной сети. Анализ исторической информации за длительный период времени (до полугода) с целью построения модели прогнозирования сбоев и атак в корпоративной сети (например, выявление увеличения числа запросов на веб-сервер и др.).

6. Выявление вредоносного зашифрованного трафика. В [7] предложены методы моделирования и представления зашифрованных соединений из логов веб-коммуникаций. Идея основана на внедрении коммуникационных шаблонов активности отдельных пользователей, которые моделируют контекстуальную информацию зашифрованных запросов. Впоследствии авторами разработаны статистические

показатели коммуникационных шаблонов, которые могут быть использованы различными алгоритмами машинного обучения, как с обучением, так и без.

- Машинное обучение в системах обнаружения вторжений нового поколения можно использовать как для автоматического обнаружения уже известных угроз, так и для обнаружения не замеченных ранее вариаций известных угроз. Алгоритмы машинного обучения могут обучаться идентифицировать необычные модели поведения в больших объемах сетевого трафика и автоматически предупреждать группы по обеспечению безопасности о необходимости дальнейшего исследования угрозы. Также они могут ускорить процесс расследования киберпреступления за счет обработки большого количества исходных данных, а в будущем осуществлять данный процесс автоматически.

Литература

1. Machine learning in cybersecurity will boost big data, intelligence, and analytics spending. URL = https://www.helpnetsecurity.com/2017/01/31/machine-learning-cybersecurity/. Дата обращения: 10.05.2018.
2. Cisco 2018. Годовой отчет по информационной безопасности. URL = https://www.cisco.com/c/dam/global/ru_ru/assets/offers/assets/cisco_2018_acr_ru.pdf. Дата обращения: 11.05.2018.
3. *Christian Callegari, Stefano Giordano, Michele Pagano* Entropy-based network anomaly Detection // 2017 International Conference on Computing, Networking and Communications (ICNC). 2017.
4. *Idhammad M.*, *Afdel K.* & *Belouch M.*, Semi-supervised machine learning approach for DDoS detection // Appl. Intell. 2018. URL = https://doi.org/10.1007/s10489-018-1141-2.
5. *Kwon D.*, *Kim H.*, *Kim J. et al*. A survey of deep learning-based network anomaly detection // Cluster Comput. 2017. URL = https://doi.org/10.1007/s10586-017-1117-8.
6. *Eric M. Hutchins*, *Michael J. Cloppert*, *Rohan M. Amin* Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin Corporation. 2010.
7. *Jan Kohout, Tomasÿ Komarek, Prÿemysl Cÿech, Jan Bodnar, Jakub Lokocÿ* Learning communication patterns for malware discovery in HTTPs data // Expert Systems With Applications. 2018.

Поступила 3 августа 2018 г.

Application of machine learning algorithms for solving information security problems

Yu.V. Vinogradov – Head of Department, LLC «SSEC-Service» (Moscow)
E-mail: vinogradov_yv@ssec.ru
A.N. Nazarov – Dr.Sc.(Eng.), Professor, FRC «Computer Science and Control» of RAS (Moscow)
E-mail: a.nazarov06@bk.ru
A.K. Sychev – Leading Mathematic Engineer, LLC «SSEC-Service» (Moscow)
E-mail: sychev_a_k@mail.ru

The article studies the use of machine learning algorithms in solving information security problems, namely, in the construction of next-generation intrusion detection systems (IDS). The main drawbacks of traditional IDS (based on signature rules) are considered and methods for their solution are proposed using the algorithms of machine learning. The article presents new methods of applying machine learning algorithms, with the help of which it is possible to detect both already known threats and previously not seen variations of known threats. They can also speed up the process of investigating cybercrime by processing a large number of source data, and in the future, carry out this process automatically.

References

1. Machine learning in cybersecurity will boost big data, intelligence, and analytics spending. URL = https://www.helpnetsecurity.com/2017/01/31/machine-learning-cybersecurity/. Data obrashheniya: 10.05.2018.
2. Cisco 2018. Godovoj otchet po informaczionnoj bezopasnosti. URL = https://www.cisco.com/c/dam/global/ru_ru/assets/offers/assets/cisco_2018_acr_ru.pdf. Data obrashheniya: 11.05.2018.
3. *Christian Callegari, Stefano Giordano, Michele Pagano* Entropy-based network anomaly Detection // 2017 International Conference on Computing, Networking and Communications (ICNC). 2017.
4. *Idhammad M.*, *Afdel K.* & *Belouch M.*, Semi-supervised machine learning approach for DDoS detection // Appl. Intell. 2018. URL = https://doi.org/10.1007/s10489-018-1141-2.
5. *Kwon D.*, *Kim H.*, *Kim J. et al.* A survey of deep learning-based network anomaly detection // Cluster Comput. 2017. URL = https://doi.org/10.1007/s10586-017-1117-8.
6. *Eric M. Hutchins*, *Michael J. Cloppert*, *Rohan M. Amin* Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin Corporation. 2010.
7. *Jan Kohout, Tomasÿ Komarek, Prÿemysl Cÿech, Jan Bodnar, Jakub Lokocÿ* Learning communication patterns for malware discovery in HTTPs data // Expert Systems With Applications. 2018.

УДК 004

Психологические аспекты информационной безопасности в эпоху больших данных[1]

Е.А. Михеев – соискатель, Институт психологии РАН (Москва)
E-mail: mih-news@mail.ru
Т.А. Нестик – д.псих.н., профессор РАН, зав. лабораторией, Институт психологии РАН (Москва)
E-mail: nestik@ipras.ru

Рассмотрены проблемы психологической безопасности, связанные с внедрением технологий анализа больших данных. Проанализированы информационно-психологические угрозы, связанные с использованием личных данных пользователей социальных сетей для манипуляции массовым сознанием и больших данных при проведении психологических и кибероперациий. Обоснован вывод о том, что при разработке механизма минимизации возникающих рисков необходимо учитывать индивидуально-психологические и социально-психологические характеристики объектов воздействия (целевой аудитории) и субъектов обеспечения информационной безопасности (специалистов по информационной безопасности).

Ключевые слова: *большие данные, цифровые следы, манипуляция, массовое сознание, информационная безопасность, психологическая операция.*

Problems of psychological security in era of Big Data analysis are discussed. Information-psychological threats such as using personal data of social network users for mass consciousness manipulation, using Big Data in information operations (IO), psychological operations (PsyOP) and cyber operations were analyzed. It is concluded that during development of mechanism to minimize emerging risks individual psychological and sociopsychological traits of target audience and subjects of information security support (experts in information security) should be taken into account.

Keywords: *Big Data, digital footprints, manipulation, mass consciousness, information security, PsyOP.*

DOI: 10.18127/j20729472-201804-06

Все более широкое внедрение анализа больших данных сопряжено с ростом вероятности использования личных данных пользователей социальных сетей для манипуляции массовым сознанием и использования больших данных при проведении информационных, психологических и кибероперациий. Возникают новые угрозы для «информационно-психологической безопасности» – состояния защищенности индивидуальных и коллективных социальных субъектов различных уровней общности от воздействия информационных факторов, вызывающих дисфункциональные социальные процессы [1].

Цель работы – рассмотреть проблемы психологической безопасности, связанные с внедрением технологий анализа больших данных.

Использование личных данных пользователей социальных сетей для манипуляции массовым сознанием

Технологии анализа цифровых следов как маркеров психологических характеристик были разработаны при изучении сообщений блогеров в Twitter и опирались преимущественно на компьютерную лингвистику. Прорывом в этой области стало сопоставление личных страниц в Facebook с ответами их владельцев на стандартизированные психологические опросники, осуществленное в рамках проекта MyPersonality.org, работы Психометрического центра Кембриджского университета и проекта «World Well-Being Project» Центра позитивной психологии Университета Пенсильвании. Начав в 2007 г. с рассылки приглашения 150 друзьям в социальной сети, М. Косинский и Д. Стилвелл за четыре года методом снежного кома собрали более 6 млн участников исследования [9]. Уже к 2013 г. им удалось обеспечить прогностическую валидность отметок «like» для шкал пятифакторной модели личности Big Five до 0,43, а при оценке политических убеждений и социально-демографических характеристик коэффициенты составляли от 0,7 до 0,9 [8]. Оказалось достаточно информации всего о 70 лайках, сделанных человеком в Facebook, чтобы предсказывать его политические предпочтения, отношение к здоровью и алкоголю

[1] Исследование выполнено по гранту РНФ №18-18-00439 «Психология человека в условиях глобальных рисков».

точнее, чем это делают его сослуживцы, а информация о 300 лайках позволяет делать это лучше, чем его жена или муж [11]. Проведенный в 2017 г. мета-анализ исследований, посвященных связи цифровых следов с «Большой Пятеркой», показывает, что их предсказательная сила колеблется от 0,29 для доброжелательности до 0,40 для экстраверсии, то есть не уступает стандартизированным опросникам [7]. Разработаны алгоритмы, позволяющие судить об уровне интеллекта, удовлетворенности жизнью, склонности к самораскрытию и самомониторингу, ценностных ориентациях личности и характеристиках временной перспективы.

Для психологического профилирования личности используются не только лингвистические маркеры и сетевой анализ, но и фотографии, размещенные на страницах Instagram и Facebook, видеозаписи, аудиозаписи речи, видеоблоги и данные смартфонов.

Полученные таким образом данные все чаще используются для повышения уровня манипуляции массовым сознанием. Примером тому может служить недавний скандал вокруг специализирующейся на психологическом профилировании по цифровым следам компании Cambridge Analytica, которую обвинили в незаконном получение доступа к 50 млн личных страниц Facebook [10] и вмешательстве во внутриполитический процесс США и Англии в ходе избирательной кампании Д. Трампа и проведении Brexit.

Профилирование личности по цифровым следам было использовано коммерческой организацией по управлению предвыборными кампаниями под названием «Лаборатория стратегических коммуникаций» (Strategic Communications Laboratories). Некоторые официальные источники указывают на то, что эта организация способствовала созданию кризисных ситуаций в развивающихся странах, участвовала в разработке для НАТО методов психологических манипуляций гражданами Афганистана.

Эта же методология была использована в ходе Brexit в Великобритании и предвыборной кампании Д. Трампа организацией Cambridge Analytica. В основе действий Cambridge Analytica лежали психологический поведенческий анализ, основанный на сопоставлении действий в социальных сетях с персональными данными пользователей, и таргетированная реклама. Эффективность такого узконаправленного информационного воздействия позднее была подтверждена М. Косинским в ходе экспериментов: было установлено, что готовность к активным действиям после получения персонифицированной информации возрастает на 1400%. Таким образом, доказана эффективность использования личных данных пользователей для повышения уровня манипуляции в социальных медиа.

Использование больших данных при проведении информационных, психологических и кибероперациий

В последнее время технологии Big Data активно используются при подготовке и проведении специальных мероприятий военизированными организациями различных государств. Так, для повышения эффективности деятельности киберподразделений и подразделений информационной и психологической борьбы разрабатываются специальные программы анализа, слежения и прогнозирования социальных, политических, информационных и экономических процессов в конкретных регионах. В частности, в США запущены: проект GDELT – Дестрометр, который был апробирован в период 2014−2016 гг. для анализа и прогнозирования гражданских ненасильственных и вооруженных конфликтов, революций, мятежей и переворотов; проект «Plan-X» по созданию аппаратно-программного комплекса (АПК), позволяющего объединять множество вредоносных программ, разрабатываемых сторонними организациями, и внедренного в работу Киберкомандования США в 2017 г. [2].

Об использовании больших массивов информации при анализе аудитории косвенно говорится и в Доктрине психологических операций НАТО [6]. В разделе повышения эффективности планирования операций с учетом специфики целевой аудитории закреплены основные принципы анализа, направленного на систематическое изучение людей с целью улучшения понимания и определения доступности, уязвимости и восприимчивости к поведенческому и установочному воздействию. В документе дана классификация информации, получаемой при анализе целевой аудитории (Target audience analysis (TAA)) в зависимости от ее характеристик.

К анализу *1 уровня* (Tier 1 TAA) относится исследование, содержащее большее количество подробностей, информации, полученной из множества источников, научно обоснованной, собранной диагностическими методами непосредственно в стране на местном языке. Информация первой категории получается из методически корректно собранных данных, проверенных на соответствие научным гипотезам.

Примером «Tier 1 TAA» является шестимесячный проект в определенной стране с привлечением исследовательской группы.

Анализом *2 уровня* (Tier 2 TAA) являются исследования, проводимые с аудиторией, которая не владеет научно обоснованными дедуктивными методами. Исследование может быть проведено непосредственно в стране или удаленно и являться по сути «оценочным». Результатом «Tier 2 TAA» является информация, записанная в ходе взаимодействия с целевой аудиторией. Примером «Tier 2 TAA» может быть вопрос солдата в адрес местного пекаря о том, что он думает по поводу того, как будут вести себя его соседи в особой ситуации.

Анализом *3 уровня* (Tier 3 TAA) являются исследования, которые содержат мало подробностей, вторичную информацию. Результатом «Tier 3 TAA» является предположение. Примером анализа 3 уровня является Интернет-исследование специфических объектов.

Из документа видно, что информация, получаемая из Интернета, относится к самому низшему уровню анализа. Однако недавние социально-психологические исследования показывают [11], что компьютерные оценки людей, основанные на цифровых следах, более точны и достоверны, чем суждения, сделанные их близкими или знакомыми (друзьями, семьей, супругом, коллегой и т.д.). Было установлено, что личностные характеристики пользователей социальных сетей могут выявляться автоматически специальной программой без участия человека.

Надо отметить, что в ходе кибероперациий технологии Big Data являются объектом атак и взлома. Целью таких атак обычно является получение доступа к важной информации.

Типичная кибератака проводится с помощью специальных аппаратных средств, включающих в себя модели, внедренные на киберобъекты [5]. Программные средства кибератак состоят из средств доставки боевой части (БЧ) кибероружия, сокрытия и управления ею, самой БЧ (боевого программного агента).

Боевая часть кибероружия состоит из программных модулей вредоносного содержания с определенным функциональным алгоритмом. Средствами доставки боевого программного агента могут быть электронные письма, веб-страницы, сервисы Интернет-ссылок, встроенная в атакующее средство микропрограмма, программное приложение или элемент аппаратных средств.

В числе уязвимостей, способствующих доставке кибероружия, помимо уязвимостей специального и прикладного ПО, операционной системы и системы безопасности, ряд исследователей называют человеческий фактор. Он активно используется при организации и проведении кибероперации. Примером могут быть кибератаки на Бушерскую АЭС и комплекс по обогащению урана в г. Натанза (Иран), которые стали возможны из-за нарушения пользователями правил информационной безопасности. Подобные нарушения тесным образом связаны с индивидуально-психологическими особенностями личности сотрудника, обеспечивающего информационную безопасность.

Исследователи отмечают, что для повышения эффективности противодействия информационным угрозам необходимы системный подход и адекватные инструменты киберразведки на основе анализа больших данных [4]. Кроме того, отдельного рассмотрения требует изучение индивидуально-личностных и социально-психологических характеристик субъектов информационного процесса: от обычных пользователей Интернета до сотрудников, обеспечивающих информационную безопасность организаций.

- Информационная безопасность больших данных связана с рядом психологических аспектов. Во-первых, это наличие большого числа возможностей для манипуляции, которые способствуют формированию искаженных, неверных представлений Интернет-пользователей. Во-вторых, это нагнетание тревоги и страхов, связанных со сбором или хищением персональных данных без ведома Интернет-пользователей. В-третьих, социально-психологические и демографические показатели больших социальных групп и общества в целом, измеряемые при анализе целевой аудитории в ходе подготовки и проведения информационной, психологической и кибероперации, могут использоваться для формирования ложного Мы-образа у целевых групп, ошибочного представления о настроениях большинства. В-четвертых, это провокация чувства беспомощности у конкретных Интернет-пользователей, ставших мишенями информационного воздействия. Учет личностных

особенностей того или иного Интернет-пользователя облегчает в дальнейшем сфокусированные, адресные информационные атаки. Интернет-пользователь, в том числе специалист по обеспечению информационной безопасности организации, попадает в ситуацию информационной асимметрии, когда о нем известно предположительно все, а для него самого источник атаки выступает обезличенной силой. В эпоху больших данных дальнейшее обеспечение информационно-психологической безопасности требует создания облачных сервисов, которые при обращении пользователя помогали бы ему оценить, каковы реальные риски использования злоумышленниками его цифровых следов, и получить поддержку для выбора стратегии защиты.

Литература

1. *Грачев Г.В.* Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. М.: Изд-во РАГС. 1998. 125 с.
2. *Карасев П.А.* США наращивают киберсилы // Журнал «Эксперт». Январь 2018. URL = http: //expert.ru/2017/08/2/ssha-naraschivayut-kibersilyi/ (дата обращения 21.06.2018).
3. *Пилипенко В.Ф.* Безопасность: теория, парадигма, концепция, культура. Словарь-справочник. Изд. 2-е, доп. и перераб. М.: ПЕР СЭ-Пресс. 2005. 192 с.
4. *Черняк Л.* Безопасность больших данных // Открытые системы СУБД. 2013. № 2. URL = https://www.osp.ru/os/2013/02/13034551 (дата обращения 21.07.2018).
5. *Якупов В.*, *Смирнов И.* Противоборство в киберпространстве: направления развития сил и средств // Журнал «Зарубежное военное обозрение». 2018. № 3. С. 13−18.
6. Allied Joint Doctrine for Psychological Operations. AJP-3.10.1. September 2014. URL = https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf (дата обращения 21.06.2018).
7. *Azacur D.*, *Settani M.*, *Marengo D.* Predicting the Big 5 personality traits from digital footprints on social media: A meta-analysis // Personality and Individual Differences. 2018. № 124. P. 150−159. URL = https://www.researchgate.net/publication/321965757_Predicting_the_Big_5_personality_traits_from_digital_footprints_on_social_media_A_meta-nalysis (дата обращения 21.07.2018).
8. *Kosinski M.*, *Stillwell D.*, *Graepel T.* Private traits and attributes are predictable from digital records of human behavior // Proc. of the National Academy of Sciences of the United States of America. PNAS. 2013. № 110. P. 5802−5805. URL = http://dx.doi.org/10.1073/pnas.1218772110 (дата обращения 21.07.2018).
9. *Kosinski M.*, *Matz S.C.*, *Gosling S.D.*, *Popov V.*, *Stillwell D.* Facebook as a research tool for the social sciences: Opportunities, challenges, ethical considerations, and practical guide // American Psychologist. 2015. № 70. P. 543−556. URL = http://dx.doi.org/10.1037/a0039210 (дата обращения 21.07.2018).
10. *Rosenberg M.* Cambridge Analytica, Trump-Tied Political Firm, Offered to Entrap Politicians // The New York Times. March, 20.2018. P. 1. URL = https://www.nytimes.com/2018/03/19/us/cambridge-analytica-alexander-nix.html (дата обращения 21.07.2018).
11. *Youyou W.*, *Kosinski M.*, *Stillwell D.* Computer-based personality judgments are more accurate than those made by humans // PNAS. January 27, 2015. URL = http://www.pnas.org/content/112/4/1036.full (дата обращения 21.07.2018).

Поступила 3 августа 2018 г.

Psychological aspects of informational security in the age of Big Data

E.A. Mikheev – Post-graduate Student, Institute of psychology of RAS (Moscow)
E-mail: mih-news@mail.ru
T.A. Nestik – Dr.Sc.(Psych.), Professor of RAS, Head of Laboratory, Institute of psychology of RAS (Moscow)
E-mail: nestik@ipras.ru

Problems of psychological security in era of Big Data analysis are discussed. Information-psychological threats such as using personal data of social network users for mass consciousness manipulation, using Big Data in information operations (IO), psychological operations (PsyOP) and cyber operations were analyzed. It is concluded that during development of mechanism to minimize emerging risks individual psychological and sociopsychological traits of target audience and subjects of information security support (experts in information security) should be taken into account.
The research is supported by a grant of the Russian Science Foundation (project № 18-18-00439 «Psychology of human beings in conditions of global risks»).

References

1. *Grachev G.V.* Informatsionno-psikhologicheskaya bezopasnost' lichnosti: sostoyanie i vozmozhnosti psikhologicheskoi zashchity. M.: Izd-vo RAGS. 1998. 125 p.
2. *Karasev P.A.* SShA narashchivayut kibersily // Zhurnal «Ekspert». Yanvar' 2018. URL = http://expert.ru/2017/08/2/ssha-naraschivayut-kibersilyi/ (data obrashcheniya 21.06.2018).
3. *Pilipenko V.F.* Bezopasnost': teoriya,paradigma, kontseptsiya, kul'tura. Slovar'-spravochnik. Izd. 2-e, dop. i pererab. M.: PER SE-Press. 2005. 192 p.
4. *Chernyak L.* Bezopasnost' bol'shikh dannykh // Otkrytye sistemy SUBD. 2013. №2. URL = https://www.osp.ru/os/2013/02/13034551 (data obrashcheniya 21.07.2018).
5. *Yakupov V., Smirnov I.* Protivoborstvo v kiberprostranstve: napravleniya razvitiya sil i sredstv // Zhurnal «Zarubezhnoe voennoe obozrenie». 2018. №3. P. 13–18.
6. Allied Joint Doctrine for Psychological Operations. AJP-3.10.1. September 2014. URL = https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf (data obrashcheniya 21.06.2018).
7. *Azacur D.*, *Settani M.*, *Marengo D.* Predicting the Big 5 personality traits from digital footprints on social media: A meta-analysis // Personality and Individual Differences. 2018. № 124. P. 150–159. URL = https://www.researchgate.net/publication/321965757_Predicting_the_Big_5_personality_traits_from_digital_footprints_on_social_media_A_meta-nalysis (data obrashcheniya 21.07.2018).
8. *Kosinski M.*, *Stillwell D.*, *Graepel T.* Private traits and attributes are predictable from digital records of human behavior // Proc. of the National Academy of Sciences of the United States of America. PNAS. 2013. № 110. P. 5802–5805. URL = http://dx.doi.org/10.1073/pnas.1218772110 (data obrashcheniya 21.07.2018).
9. *Kosinski M.*, *Matz S.C.*, *Gosling S.D.*, *Popov V.*, *Stillwell D.* Facebook as a research tool for the social sciences: Opportunities, challenges, ethical considerations, and practical guide // American Psychologist. 2015. № 70. P. 543–556. URL = http://dx.doi.org/10.1037/a0039210 (data obrashcheniya 21.07.2018).
10. *Rosenberg M.* Cambridge Analytica, Trump-Tied Political Firm, Offered to Entrap Politicians // The New York Times. March, 20.2018. P. 1. URL = https://www.nytimes.com/2018/03/19/us/cambridge-analytica-alexander-nix.html (data obrashcheniya 21.07.2018).
11. *Youyou W.*, *Kosinski M.*, *Stillwell D.* Computer-based personality judgments are more accurate than those made by humans // PNAS. January 27, 2015. URL = http://www.pnas.org/content/112/4/1036.full (data obrashcheniya 21.07.2018).

УДК 004.9

Разработка методов автоматического анализа социальных сетей для обеспечения безопасности организации

С.С. Мигалин – ассистент, НИУ ВШЭ (Москва)
E-mail: sergey@migalin.ru
М.А. Коврижных – ассистент, НИУ ВШЭ (Москва)
E-mail: makovrizhnykh@gmail.com
А.Б. Лось – к.ф.-м.н., доцент, НИУ ВШЭ (Москва)
E-mail: alos@hse.ru

Рассмотрены вопросы разработки автоматической системы для анализа пользователей социальных сетей по различным признакам. Предложено алгоритмическое решение, включающее в себя разработку ряда отдельных модулей. Разработанная система протестирована на реальных примерах и может быть рекомендована, в частности, кадровым службам организации и службам безопасности для получения информации о действующих сотрудниках и сотрудниках, принимаемых на работу.

Ключевые слова: *социальные сети, комплекс программ, персональные страницы пользователей, сообщества социальной сети, запрещенный контент.*

The paper deals with the development of an automatic system for the analysis of users of social networks on various grounds. An algorithmic solution is proposed, including the development of a number of separate modules. The developed system is tested on real examples and can be recommended, in particular, to personnel services of the organization and security services to obtain information about existing employees and employees hired.

Keywords: *social networking, software personal user pages, community, social network, prohibited content.*

DOI: 10.18127/j20729472-201804-07

Ц е л ь р а б о т ы – рассмотреть задачу разработки методов анализа социальных сетей для получения информации о личностных качествах принимаемых на работу специалистов или уже работающих в организации сотрудников. В последнее время общение в соцсетях и обмен в них всевозможной информацией стал очень популярен среди граждан нашей страны [1−3]. Содержательный анализ указанной информации может дать весьма полезные сведения о лицах, интересующих кадровые службы и службы безопасности организации.

В ходе решения задачи разработан комплекс программ для анализа персональных страниц пользователей социальных сетей, различных сообществ и сайта федеральной службы судебных приставов. Разработано соответствующее приложение и проведено тестирование его работы на реальных страницах пользователей и активно действующих сообществах социальной сети, в частности, сообществ, связанных с ведущими университетами России, а также на персональных страницах сотрудников энергетической компании.

По данным ВЦИОМ, самой популярной социальной сетью среди россиян в 2017 г. является «Вконтакте» [4]. В процессе изучения существующих разработок для автоматического анализа был найден ряд инструментов [5−9]. Однако анализ показал, что они имеют узкую направленность, высокую стоимость и невозможность модификации из-за недоступности исходного кода.

Разработка системы анализа

С учетом недостатков существующих программ разработана кроссплатформенная система автоматического анализа с открытым исходным кодом на языке программирования Python. Для написания интерфейса был использован открытый фреймворк Qt, который позволил совместить кроссплатформенность с высокой производительностью. Для взаимодействия с сервисами социальной сети Вконтакте использована открытая библиотека vk_api (рис. 1).

Для обработки текстов постов пользователей и сообществ разработан модуль анализа текстовой информации на наличие неприемлемого содержимого, учитывающий морфологию русского языка на основе открытой библиотеки pymorphy2 (рис. 2).

Рис. 1. Главная страница приложения VKAnalysis

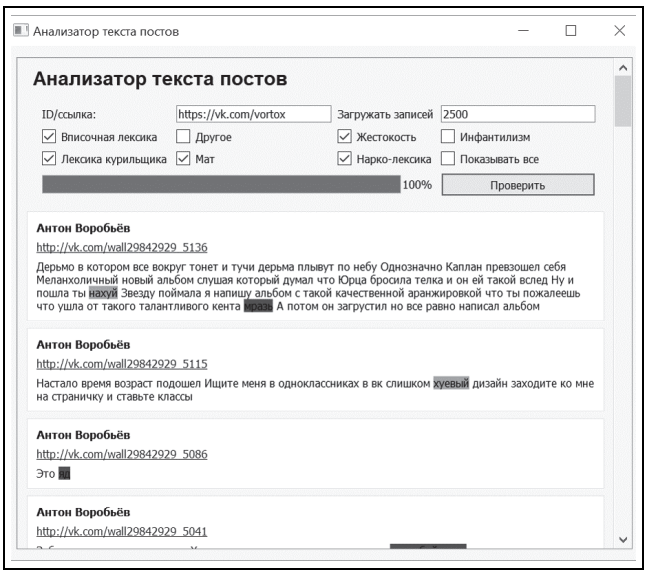

Рис. 2. Пример анализа текстовой информации страницы пользователя

Рис. 3. Пример проверки изображений на наличие NSFW-контента

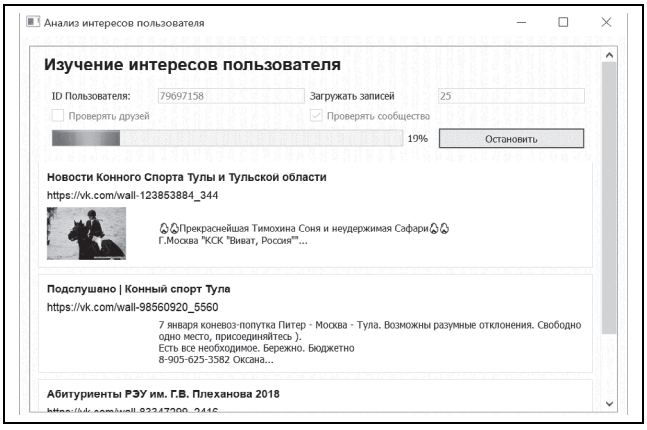

Рис. 4. Модуль изучения интересов

На основе текстов сообществ по интересам созданы словари для анализа ряда категорий, в частности: «ненормативная лексика», «курение», «наркотики», «жестокость», «инфантилизм» и «тусовки». Предусмотрена возможность простой расширяемости числа категорий, например, для анализа упоминаний компании.

Для обработки фотографий пользователей и сообществ разработан модуль определения неприемлемых (Not Suitable For Work) изображений с использованием открытой библиотеки для глубинного машинного обучения Caffe и обученной модели нейросети от Yahoo OpenNSFW [10] (рис. 3).

Для изучения индивидуальных особенностей пользователя был разработан модуль анализа пользовательской активности, включающий время, проведенное в сети, интересы, определяемые на основе исследования понравившихся публикаций, круга общения, установленного на основе эвристик и активности пользователей по отношению друг к другу (рис. 4).

Для получения актуальной информации о наличии долгов пользователя разработан модуль определения задолженностей путем анализа открытой информации сайта fssprus.ru. Произведен доступ к открытому банку данных исполнительных производств посредством интерфейса программирования приложения (API). Благодаря модульной архитектуре приложения система легко расширяема для дальнейших разработок, в том числе для построения социальных графов, проверки по дополнительным источникам (наличия правонарушений, взаимодействий с регуляторами, наличия упоминаний фамилии и имени в Интернет-ресурсах государственных органов, коммерческих или общественных организаций, профилей в других социальных сетях и т.д.).

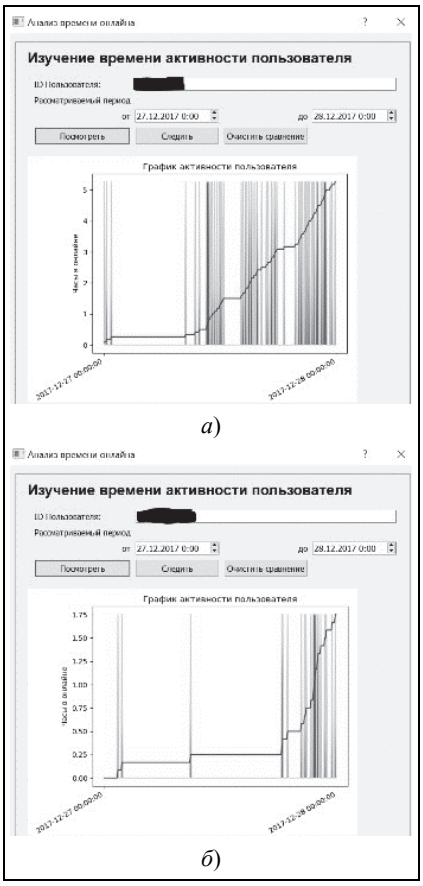

Рис. 5. Сравнение времени, проведенного в социальной сети секретарем (*а*) и коммерческим директором (*б*)

Тестирование приложения в компании ООО «ЭЛЕКТРУМ ЦЕНТР»

Разработанное приложение протестировано на страницах сотрудников компании ООО «ЭЛЕКТРУМ ЦЕНТР». Для повышения производительности труда, укрепления трудовой дисциплины, обеспечения безопасности и имиджа организации необходимо, чтобы сотрудники не использовали социальные сети во время работы, если этого не предполагают должностные обязанности, и их страницы не содержали материалов, неприемлемых для имиджа компании. Проведено тестирование времени, проведенного сотрудниками компании в социальных сетях, в период с 25 по 29 декабря 2017 г. Результаты представлены на рис. 5.

По результатам тестирования были выявлены сотрудники, которые проводили много времени в социальных сетях на рабочем месте. Сотрудников, публикующих неприемлемые для имиджа компании материалы, выявлено не было.

Тестирование приложения для анализа групп, связанных с университетами РФ

Приложение было протестировано на сообществах, которые связаны с именами крупных университетов страны. Для исследования выбраны следующие университеты: МГУ, МИФИ, Высшая школа экономики, СПбГУ, МФТИ, РЭУ им. Плеханова. Кроме того, выбраны три самых популярных сообщества на момент исследования, в названии которых фигурировало название вуза. По результатам проверки выяснилось, что в группах «Подслушано в МГУ», «Цитаты преподавателей МГУ», «Подслушано в МИФИ», «Подслушано в СПбГУ», «Подслушано в МФТИ», «Подслушано в РЭУ им. Плеханова» содержится нецензурная брань, в группах «МГУ имени М.В. Ломоносова» – лексика, связанная с употреблением алкоголя, а неприемлемые фотографии – в группах «МИФИ», «Подслушано в МИФИ», «Команда КВН «Сборная Высшей школы экономики» ВШЭ», «Подслушано в МГУ».

- В ходе проведенных исследований разработана и протестирована система автоматического анализа персональных страниц, сообществ социальной сети и открытых данных сайта fssprus.ru. Результаты работы могут быть использованы при проведении различных социологических исследований, а также специалистами отделов кадров и службы безопасности с целью проведения мероприятий, связанных с управлением персоналом, поддержанием имиджа, контролем сотрудников и упоминаний компании в социальных сетях.

Литература

1. *Сумкин К.С.*, *Тараненко Л.О.* Анализ страницы пользователя социальной сети «ВКонтакте» // Молодой ученый. 2016. № 12(116). С. 189–194.
2. *Черемисова И.В.* Контент-анализ страниц активных пользователей социальной сети «ВКонтакте» // Вестник Волгоградского гос. ун-та. Сер. 11: Естественные науки. 2016. № 2(16). С. 74–803.
3. *Багрецов Г.И.*, *Шиндарев Н.А.*, *Абрамов М.В.*, *Тулупьева Т.В.* Подходы к автоматизации сбора, структурирования и анализа информации о сотрудниках компании на основе данных социальной сети // Труды VII Всерос. научно-практич. конф. «Нечеткие системы, мягкие вычисления и интеллектуальные технологии (НСМВИТ-2017)». 2017. С. 9–16.
4. ВЦИОМ. Пресс-выпуск № 3388 [Электронный ресурс]. URL = https://wciom.ru/index.php?id=236&uid=116254.
5. *Пащенко А.Е.*, *Тулупьева Т.В.* Экспресс-анализ реплик и метаданных социальных сетей с использованием программных средств автоматизации получения данных // Материалы Всерос. науч. конф. по проблемам информатики СПИСОК-2014. СПб. 23–25 апреля 2014. С. 563–568.

6. *Бурлуцкий В.В.* Автоматизированный анализ активностей пользователей социальных сетей для выявления общественной реакции // Вестник Югорского гос. ун-та. 2012. № 3(26). С. 62–65.
7. *Ермакова А.Ю.* Разработка методов прогнозирования на примере анализа средств вычислительной техники // Промышленные АСУ и контроллеры. 2017. № 1. С. 28–34.
8. *Donchenko D.*, *Ovchar N.*, *Sadovnikova N.*, *Parygin D.*, *Ather D.* Analysis of Comments of Users of Social Networks to Assess the Level of Social Tension // Procedia Computer Science. 2017. V. 119. P. 359–367.
9. *Yakushev A.*, *Mityagin S.* Social Networks Mining for Analysis and Modeling Drugs Usage // Procedia Computer Science. 2014. V. 29. P. 2462–2471.
10. URL = https://github.com/yahoo/open_nsfw.

Поступила 3 августа 2018 г.

Development of methods for automatic analysis of social networks to ensure the security of the organization

S.S. Migalin – Assistant, HSE (Moscow)
E-mail: sergey@migalin.ru
M.A. Kovrizhnykh – Assistant, HSE (Moscow)
E-mail: makovrizhnykh@gmail.com
A.B. Los – Ph.D.(Phys.-Math.), Associate Professor, HSE (Moscow)
E-mail: alos@hse.ru

The paper deals with the development of an automatic system for the analysis of users of social networks on various grounds. An algorithmic solution is proposed, including the development of a number of separate modules. For the analysis of textual information on pages users and communities selected algorithm lemmatization. The analysis of the photos is performed using the open library of deep machine learning Caffe. Analysis of the circle of communication is the identification of the user's friends with whom he is the most active communication. The following options are available: shared city, shared age, shared friends, likes and reposts from friends and friends. To determine the range of interests of the user, the module checks the pages of his friends, his community and looks for records on which the user has put a «like», then displays information about the record with the ability to go to it. To check the availability of the debt in the enforcement proceedings of the Federal bailiff service developed a module that allows you to look for debt of individuals from public information data Bank in the enforcement proceedings of the Federal bailiff service of Russia through the official APIs of the Federal bailiff service of the Russian Federation. The developed system is tested on real examples and can be recommended, in particular, to personnel services of the organization and security services to obtain information about existing employees and employees hired.

References

1. *Sumkin K.C., Taranenko L.O.* Analiz stranici pol'zovatelya social'noy seti «VKontakte» // Molodoy ucheniy. 2016. №12(116). S. 189–194.
2. *Chermisov I.V.* Kontent-analiz stranic aktivnikh pol'zovateley social'noy seti «VKontakte»// Vestnik Volgogradskogo gos. un-ta. Ser. 11: Estesnvennie nauki. 2016. №2(16). S. 74–803.
3. *Bagrecov G.I., Shindarev N.A., Abramov M.V., Tulup'eva T.V.* Podkhodi k avtomatizacii sbora, strukturirovaniya i analiza informacii o sotrudnikakh kompanii na osnove dannikh socialnoy seti // Trudi VII Vseros. nauchno-praktich. konf. «Nechetkie sistemi, myagkie vichisleniya I intellektual'nie tekhnologii (NCMBIT-2017)». 2017. S. 9–16.
4. VCIOM. Press-vipusk № 3388 [Elektronniy resurs]. URL = https://wciom.ru/index.php?id=236&uid=116254.
5. *Pashenko A.E., Tulup'eva T.V.* Ekspress-analiz replik i metadannikh socialnikh setey s ispolzovaniem programmnikh sredstv avtomatizacii polucheniya dannikh // Materiali Vseros. nauch. konf. po problemam informatiki SPISOK-2014. SPb. 23–25 aprelya 2014. S. 563–568.
6. *Burluckiy V.V.* Avtomatizirovanniy analiz aktivnostey polzovateley socialnikh setey dlya viyavleniya obshestvennoy reakcii // Vestnik Yugorskogo gos. un-ta. 2012. № 3(26). S. 62–65.
7. *Ermakova A.Y.* Razrabotka metodov prognozirovaniya na primere analiza sredstv vichislitelnoy tekhniki // Promishlennie ASU I kontrolleri. 2017. № 1. S. 28–34.
8. *Donchenko D.*, *Ovchar N.*, *Sadovnikova N.*, *Parygin D.*, *Ather D.* Analysis of Comments of Users of Social Networks to Assess the Level of Social Tension // Procedia Computer Science. 2017. V. 119. P. 359–367.
9. *Yakushev A.*, *Mityagin S.* Social Networks Mining for Analysis and Modeling Drugs Usage // Procedia Computer Science. 2014. V. 29. P. 2462–2471.
10. URL = https://github.com/yahoo/open_nsfw.

УДК 004.9

Подход к оценке защищенности информационной системы на основе анализа инцидентов

А.Ю. Ермакова – ст. преподаватель, РТУ МИРЭА (Москва)
E-mail: a.alla1105@mail.ru

Рассмотрен подход к оценке уровня защищенности информационной системы (ИС) на основе анализа возникших инцидентов, построения прогнозной модели их дальнейшего поведения и последующей оценке времени безопасной эксплуатации ИС. Использован предложенный автором в [10] метод построения прогнозной модели изменения состояний динамической системы, состояния которой заданы в виде табличных значений – узловых точек, который основан на построении непрерывной «аппроксимирующей» функции, наиболее близко отстоящей от узловых точек, и последующем вычислении на ее основе прогнозных значений состояния системы. Указанный метод применен для построения прогнозной модели возникновения инцидентов ИС, приводящих к нарушению ее безопасности. Показано, как на основе построенной прогнозной функции может быть вычислено время безопасной работы ИС.

Ключевые слова: *анализ инцидентов, оценка уровня защищенности, прогнозная модель, аппроксимирующие функции, сетевые атаки, веб-угрозы.*

The paper considers an approach to assessing the level of security of the information system (IS) based on the analysis of the incidents, the construction of a predictive model of their further behavior and the subsequent evaluation of the time of safe operation of the information system. Previously, the author proposed a method for constructing a predictive model of changing the States of a dynamic system, the States of which are set in the form of table values – node points. The method is based on constructing a continuous «approximation» of the function that is most distant from the nodal points and the subsequent calculation on the basis of the forecast values of the system state. In this paper, this method is used to build a predictive model of the occurrence of incidents from, leading to a violation of its security. The following shows how based on the constructed predictive function can be calculated safe operation time IS.

Keywords: *analysis of incidents, assessment of security level, predictive model, approximating functions, network attack, web threats.*

DOI: 10.18127/j20729472-201804-08

Проблема оценки уровня защищенности информационных систем (ИС) в настоящее время является весьма актуальной. С одной стороны, на них постоянно идут негативные воздействия, а с другой, организации расходуют большие средства на вопросы защиты информационных ресурсов. Все нормативные и руководящие документы по защите информации [1–3] содержат в этом вопросе весьма расплывчатые формулировки и требования. В то же время специалистами по защите информации много внимания уделяется вопросам возникновения инцидентов и, в частности, реализации злоумышленниками различных видов атак и противодействия им [4–9], а также анализу структуры атак, направленности и статистическому учету.

Ц е л ь р а б о т ы – продолжить исследования возможных подходов к оценке уровня защищенности ИС на основе предложенного ранее в статье [10] временного подхода к оценке защищенности ИС. Суть этого подхода заключается в следующем.

В классическом подходе при исследовании уровня защищенности ИС, основанном на оценке рисков, необходимо оценить величину ущерба $R_{\text{риск}}$ при успешной реализации угроз $y_1, y_2, \ldots, y_n$ в условиях, когда ущерб от реализации угрозы y_i составляет величину u_i:

$$R_{\text{риск}} = \sum_{i=1}^{n} p(y_i)u_i, \tag{1}$$

где $p(y_i)$ – вероятность успешной реализации угрозы y_i.

Далее задается некоторая граница допустимых потерь R_0 и ИС считается защищенной, если выполнено условие

$$R_{\text{риск}} \le R_0. \tag{2}$$

Однако, как нетрудно видеть, данный подход не учитывает возможность изменения во времени ни вероятности успешной реализации угрозы, ни ущерба от такой реализации.

В то же время, как отмечено в работе [10], если удается учесть зависимость величин $p(y_i)$ и u_i от времени t, то есть построить функции $p(y_i) = p(y_i,t)$ и $u_i = u_i(t)$, то условие (2) принимает вид

$$R_{\text{риск}}(t) \le R_0. \quad (3)$$

Поскольку, как правило, функция рисков $R_{\text{риск}}(t)$ является возрастающей функцией аргумента t, то корень уравнения $R_{\text{риск}}(t) = R_0$ можно рассматривать как время T_0, в течение которого ИС может безопасно эксплуатироваться.

Далее в работе на примере построения прогнозной функции появления инцидентов рассматривается возможность оценки параметра T_0.

Построение прогнозной модели появления инцидентов

Для построения прогнозной функции появления инцидентов воспользуемся предложенным в работе [11] методом, основанном на построении по таблично заданным значениям состояния динамической системы «аппроксимирующей» функции, наиболее близко отстоящей от указанных значений в метрике наименьших квадратов. Суть данного метода состоит в следующем.

Пусть на отрезке $[a, b]$ задана одномерная сетка $X = \{x_i / x_i = x_{i-1} + h_i,\ h_i > 0,\ i = 1, 2, \ldots, n;\ x_0 = a,\ x_n = b\}$, в узлах x_i которой заданы значения $y_i = f(x_i)$, $i = 0, 1, 2, \ldots, n$ – соответствующие значения функции $f(x)$. Будем далее рассматривать данную таблицу как таблицу состояний некоторой динамической системы. При этом величины x_i будут означать моменты времени при наблюдении состояния рассматриваемой системы, а величины y_i – сами эти состояния.

Пусть также для аппроксимации табличных данных выбран некоторый класс функций $F(x,c_0,c_1,\ldots,c_m)$, $m < n$, где $c_0, c_1, \ldots, c_m$ – коэффициенты, выбор значений которых позволяет определить конкретную функцию из выбранного класса. Требуется найти значения коэффициентов $c_0, c_1, \ldots, c_m$, для которых выполнено условие

$$\Phi(c_0,c_1,\ldots,c_m) = \sum_{i=0}^{n}\left[y_i - F(x_i,c_0,c_1,\ldots,c_m)\right]^2 \to \min. \quad (4)$$

Выбранные в соответствии с критерием (1) значения коэффициентов позволяют определить среди множества функций конкретную функцию, наиболее согласованную с табличными (экспериментальными) данными или, иначе говоря, обеспечивающую наилучшее среднеквадратическое приближение.

Функция $F(x,c_0,c_1,\ldots,c_m)$ называется моделью, а искомые коэффициенты $c_0, c_1, \ldots, c_m$ – параметрами модели. В дальнейшем ограничимся рассмотрением случая, когда модель линейно зависит от параметров и ее можно представить в виде

$$F(x, c_0, c_1, \ldots, c_m) = c_0\varphi_0(x) + c_1\varphi_1(x) + \ldots + c_m\varphi_m(x), \quad (5)$$

где $\varphi_0(x), \varphi_1(x), \ldots, \varphi_m(x)$ – множество так называемых базисных функций.

Базисные функции могут быть как линейными, так и нелинейными функциями переменной x. Независимо от этого модель (5) остается линейной, поскольку она линейно зависит от модельных параметров $c_0, c_1, \ldots, c_m$.

Таким образом, для линейной модели (5) требуется найти значения параметров $c_0, c_1, \ldots, c_m$, обеспечивающих выполнение условия (4).

Для построения «аппроксимирующей» функции разработано специализированное программное обеспечение, позволяющее строить указанную функцию как в ручном, так и в автоматическом режиме, и описание которого приведено в работе [11].

Рассмотрим примеры построения непрерывных «аппроксимирующих» функций по данным об инцидентах ИС, приведенным на сайте Е. Касперского [12].

В первом примере рассмотрены данные по сетевым атакам.

Сетевые атаки. Данные по сетевым атакам взяты на период с 20.10.2017 по 18.11.2017, нормирующий коэффициент 100, за нулевое значение по оси OX принята дата 01.10.2017.

«Аппроксимирующая» функция, построенная по указанным данным, имеет вид

$$F_1(x) = 86618{,}3117 - \frac{640598{,}1148}{x^2} + 48{,}1926x + 1694{,}8417\sin[x]\ . \quad (6)$$

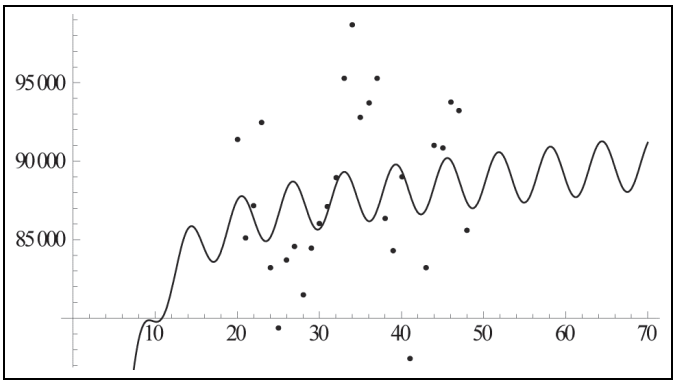

Рис. 1. График «аппроксимирующей» непрерывной функции $F_1(x)$ – прогноз сетевых атак

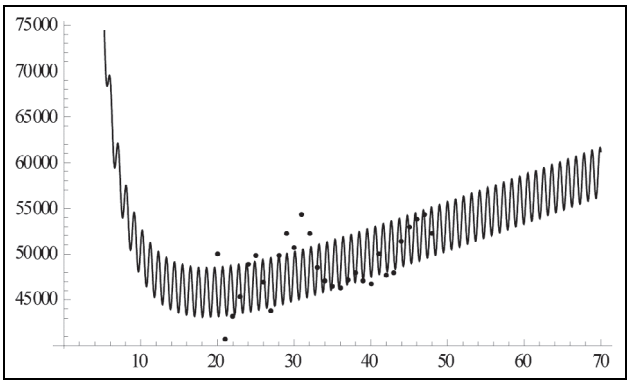

Рис. 2. График «аппроксимирующей» непрерывной функции $F_2(x)$ – прогноз Web-угроз

График функции $F_1(x)$ представлен на рис. 1.

Во втором примере использовались данные о Web-угрозах [12].

Web-угрозы. Данные по этим инцидентам взяты также на период с 20.10.2017 по 17.11.2017, нормирующий коэффициент 100, за нулевое значение по оси *OX* принята дата 01.10.2017.

«Аппроксимирующая» непрерывная функция, построенная по указанным данным, имеет вид

$$F_2(x) = 37234,4242 + \frac{990124,1754}{x^2} + 307,67881x - 2689,5393\sin\left[6x\right] . \quad (7)$$

График функции $F_2(x)$ представлен на рис. 2.

Оценка защищенности информационной системы

Покажем, как на основе полученных данных могут быть построены оценки защищенности ИС. Как видно из соотношений (6) и (7), непрерывные «аппроксимирующие» функции в том и другом случае имеют следующий общий вид: $F(x) = \alpha_1 + \alpha_2 x^{-2} + \alpha_3 x + \alpha_4 \sin(\alpha_5 x)$, где $\alpha_1, \ldots, \alpha_5$ – некоторые постоянные.

Очевидно, что при фиксированных значениях величин $\alpha_1, \ldots, \alpha_5$ функция $F(x)$ является возрастающей, при этом имеет место неравенство $F(x) \le \alpha_6 + \alpha_3 x$, где $\alpha_6 = \alpha_1 + \alpha_2 + \alpha_4$, $x \ge 1$.

Тогда, предполагая, что каждый инцидент влечет ущерб в размере u условных единиц, определив границу максимально допустимых потерь R_0 и решая уравнение $(\alpha_6 + \alpha_3 x)u = R_0$, можно получить оценку времени безопасной эксплуатации ИС:

$$T_0 = [R_0/u - \alpha_6]/\alpha_3. \quad (8)$$

Очевидно, что оценка (8) может быть уточнена в различных направлениях. В частности, могут быть построены временные модели изменения ущерба в результате возникновения инцидентов, расширен список самих инцидентов, введены весовые характеристики для учета специфики самой ИС.

Дальнейшее развитие предлагаемого подхода

В качестве направления дальнейших исследований можно указать разработку теоретико-вероятностных моделей компьютерных атак, оценку вероятности их успешного применения, а также разработку теоретико-вероятностных моделей динамики изменения стоимости активов организации и моделей возникновения ущерба при успешной реализации атак. На основе разработанных моделей можно продолжить разработку методов оценки времени безопасной эксплуатации ИС.

- Продолжено изучение актуальной проблемы, состоящей в разработке методов оценки защищенности ИС. На основе предложенного ранее временного подхода к указанной проблеме предлагается проведение анализа возникающих инцидентов, построение на его основе непрерывной «аппроксимирующей» временной функции и последующее вычисление времени безопасной эксплуатации данной системы. Приведены примеры реализации данного подхода на основе данных об инцидентах Лаборатории Касперского. Отмечены направления дальнейшего развития данного подхода.

Литература

1. ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.
2. Федеральный закон от 26 июля 2017 г. № 187 – ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
3. Экспертиза и аудит информационной безопасности. [Электронный ресурс]. URL = sudexpa.ru/expertises/ekspertiza-i-audit-informatcionnoi-bezopasnosti/ (дата обращения 17.02.2018).
4. Аудит информационных систем. Регола-мониторинг. [Электронный ресурс]. URL = spb.systematic.ru/about/news/regola-monitoring.htm (дата обращения 20.02.2018).
5. Обзор рынка SIEM-систем. [Электронный ресурс]. URL = www.antimal ware.ru/node/11 637 (дата обращения 15.03.2018).
6. *Шелухин О.И.*, *Сакалема Д.Ж.*, *Филинова А.С.* Обнаружение вторжений в компьютерные сети. М.: Горячая линия – Телеком. 2013. 220 с.
7. *Лукацкий А.В.* Обнаружение атак. СПб.: БХВ-Петербург. 2003. 596 с.
8. *Vaidya J.*, *Clifton C.* Privacy-preserving outlier detection // Proc. of the 4th IEEE International Conference on Data Mining. 2004. P. 233–240.
9. *Zimmermann J.*, *Mohay G.* Distributed intrusion detection in clusters based on non-interference // Proc. of the Australasian Workshops on Grid Computing and E-Research (ACSW Frontiers). Australian Computer Society, Inc. 2006. P. 89–95.
10. *Кабанов А.С.*, *Лось А.Б.*, *Трунцев В.И.* Временная модель оценки риска нарушения информационной безопасности // Доклады ТУСУР. Томск. 2012. № 1. Ч. 2. С. 87–91.
11. *Ермакова А.Ю.* Разработка методов прогнозирования на примере анализа средств вычислительной техники // Промышленные АСУ и контроллеры. 2017. № 1. С. 28–34.
12. Сайт Лаборатории Касперского. [Электронный ресурс]. URL = https://securelist.ru/ statistics/ (дата обращения 27.03.2018).

Поступила 3 августа 2018 г.

Approach to the assessment of information system security, based on the analysis of incidents

A.Yu. Ermakova – Senior Lecturer, RTU MIREA (Moscow)
E-mail: a.alla1105@mail.ru

The paper considers an approach to assessing the level of security of the information system (IS) based on the analysis of the incidents, the construction of a predictive model of their further behavior and the subsequent evaluation of the time of safe operation of the information system. Previously, the author proposed a method for constructing a predictive model of changing the States of a dynamic system, the States of which are set in the form of table values – node points. The method is based on constructing a continuous «approximation» of the function that is most distant from the nodal points and the subsequent calculation on the basis of the forecast values of the system state. In this paper, this method is used to build a predictive model of the occurrence of incidents from, leading to a violation of its security. The following shows how based on the constructed predictive function can be calculated safe operation time IS. Examples of this approach are given on the basis of data on Kaspersky Lab's incidents. The directions of further development of this approach are noted.

References

1. GOST R ISO/MEK 27000-2012 Informacionnaya tekhnologiya (IT). Metodi i sredstva obespecheniya bezopasnosti. Sistemi menedgmenta informacionnoy bezopasnosti.
2. Federal'niy zakon ot 26 iulya 2017 g. № 187 – FZ «O bezopasnosti kriticheskoy informacionnoy infrastruktyri Rossiyskoy Federacii».
3. Ekspertiza i audit informacionnoy bezopasnosti. [Elektronniy resurs]. URL = sudexpa.ru/expertises/ekspertiza-i-audit-informatcionnoi-bezopasnosti/ (Data obrasheniya 17.02.2018).
4. Audit informacionnikh sistem. Regola-monitoring. [Elektronniy resurs]. URL = spb.systematic.ru/about/news/regola-monitoring.htm (Data obrasheniya 20.02.2018).
5. Obzor rinka SIEM-sistem. [Elektronniy resurs]. URL = www.antimal ware.ru/node/11 637 (Data obrasheniya 15.03.2018).
6. *Shelukhin O.I., Sakalema D.G., Filinova A.S.* Obnarugenie vtorgeniy v komp'uternie seti. M.: Goryachaya liniya – Telekom. 2013. 220 s.
7. *Lukackiy A.V.* Obnarugenie atak. SPb.: BKhV-Peterburg. 2003. 596 s.
8. *Vaidya J., Clifton C.* Privacy-preserving outlier detection // Proc. of the 4th IEEE International Conference on Data Mining. 2004. P. 233–240.
9. *Zimmermann J., Mohay G.* Distributed intrusion detection in clusters based on non-interference // Proc. of the Australasian Workshops on Grid Computing and E-Research (ACSW Frontiers). Australian Computer Society, Inc. 2006. P. 89–95.
10. *Kabanov A.S., Los A.B., Trunev V.I.* Vremennaya model ocenki riska narusheniya informacionnoy bezopasnosti // Dokladi TUSUR. Tomsk. 2012. № 1. Ch. 2. S. –91.
11. *Ermakova A.Y.* Razrabotka metodov prognozirovaniya na primere analiza sredstv vichislitelnoy tekhniki // Promishlennie ASU i kontrolleri. 2017. № 1. S. 28–34.
12. Sait Laboratorii Kasperskogo. [Elektronniy resurs]. URL = https://securelist.ru/ statistics/ (Data obrasheniya 27.03.2018).

УДК 004.62

Реализация методов интеграции данных в хранилище для поддержки поисково-спасательных операций в Арктической зоне

Д.О. Брюхов – к.т.н., ст. науч. сотрудник, Институт проблем информатики ФИЦ ИУ РАН (Москва)
E-mail: dbriukhov@ipiran.ru
Н.А. Скворцов – науч. сотрудник, Институт проблем информатики ФИЦ ИУ РАН (Москва)
E-mail: nskv@ipi.ac.ru
С.А. Ступников – к.т.н., ст. науч. сотрудник, Институт проблем информатики ФИЦ ИУ РАН (Москва)
E-mail: sstupni-kov@ipiran.ru

Рассмотрен подход к реализации методов интеграции данных по Арктической зоне в единое хранилище, а именно: методов извлечения структурированных данных из текстовых документов; преобразования данных к схеме хранилища; слияния данных из разных источников для образования интегрированных представлений; верификации программ интеграции данных; реализации хранилища; загрузки интегрированных данных в хранилище данных. Описаны примеры аналитических запросов над единой схемой хранилища, которые могут быть использованы для планирования поисково-спасательных операций (ПСО).

Ключевые слова: *интеграция данных, платформы распределенного хранения и обработки данных, поиск и спасание, Арктика.*

This paper presents an approach for implementation of methods for data integration into a unified warehouse. In particular, the following issues are considered: extraction of structured data from text documents, transformation of data into warehouse schema, fusion of data from various sources to create integrated entities, data integration program verification, warehouse implementation, loading of integrated data into the warehouse. Examples of analytical queries over warehouse schema that can be used for planning of search and rescue operations are presented.

Keywords: *data integration, software frameworks for distributed data storage and processing, search and rescue operations, Arctic.*

DOI: 10.18127/j20729472-201804-09

Ввиду значительного разнообразия источников данных по Арктической зоне, которые могут быть использованы для планирования поисково-спасательных операций (ПСО) [1], задача разработки методов интеграции данных в этой предметной области представляется весьма актуальной. В работе [2] авторами была предложена масштабируемая архитектура системы извлечения информации из данных по Арктической зоне. Архитектура основана на платформе Apache Hadoop [3], обеспечивающей распределенное хранение и параллельную обработку информации. Данные хранятся в распределенной файловой системе HDFS [3], которая может располагаться на множестве физических серверов и ориентирована на работу с файлами большого объема. При работе со всем многообразием информации, применимой для планирования ПСО, разноструктурированные данные заранее извлекаются из различных источников, интегрируются и помещаются в единое хранилище для поддержки поисковых действий. Структуры информации, составляющие схему хранилища, были исследованы и описаны авторами в работе [4]. Структуры были выделены на основании используемых для Арктической зоны стандартов и форматов данных, а также данных, содержащихся в различных информационных системах. Схема хранилища является целевой для процесса интеграции, преобразующего данные из различных источников в структуры, удовлетворяющие схеме хранилища. Схема хранилища содержит набор сущностей, связанных с описанием поисковых операций, поисковых задач и инцидентов, сил и средств в составе координационных центров ПСО, объектов поиска, маршрутов, траекторий движения, а также инфраструктуры портов и аэродромов, средств коммуникации, локации и оповещения, погодных условий, упоминаний инцидентов и объектов поиска в сети Интернет и СМИ.

В качестве системы управления базами данных (СУБД) для реализации хранилища интегрированных данных в архитектуре предложена масштабируемая распределенная среда вычислений Apache Hive [5], проецирующая структуру на данные, хранимые в распределенной файловой системе HDFS. Использование Hive в архитектуре хранения и обработки структурированных данных предполагает, что струк-

турированные данные собраны из различных источников, а аналитические задачи могут формулироваться с использованием SQL-подобного языка HiveQL. HiveQL поддерживает основные типы данных SQL и расширяет их сложными типами, такими как MAP, LIST, STRUCT. Запросы на нем компилируются и выполняются как задания MapReduce [6] над наборами данных в распределенной файловой системе HDFS.

Также в работе [2] были предложены методы интеграции разноструктурированных данных для извлечения информации, нацеленной на поддержку ПСО. В работе [7] предложен и программно реализован подход к верификации программ интеграции данных, то есть их формальной проверки на соответствие заданным требованиям.

Цель работы – описать подход к реализации предложенных ранее методов интеграции данных по Арктической зоне в единое хранилище. В качестве конкретных источников данных, подлежащих интеграции, выбраны: система мониторинга судов (СМС) «Виктория» [8]; комплексная интегрированная информационная система «МоРе» [9]; межведомственная информационная система ЕСИМО [10]; международная спутниковая поисково-спасательная система КОСПАС-САРСАТ [11]; программный комплекс «Поиск-Море» [12].

Реализованный процесс интеграции данных включает в себя следующие этапы:

Этап 1. *Извлечение структурированных данных из текстовых документов*.

Этап 2. *Загрузка данных* из отобранных источников в файловую систему HDFS в исходных форматах источников.

Этап 3. *Приведение данных*, полученных от исходных источников, *к единому формату* (используется формат JSON [13]).

Этап 4. *Преобразование данных* к схеме хранилища, что позволяет однотипно работать с разнородными данными различных исходных коллекций.

Этап 5. *Слияние данных* из разных источников для образования интегрированных представлений информации об одной и той же сущности реального мира.

Этап 6. *Верификация программ интеграции данных.*

Этап 7. *Загрузка интегрированных данных в хранилище данных*. Хранилище данных, как это предусмотрено архитектурой, реализовано на основе системы Apache Hive.

В статье описаны и проиллюстрированы на примерах упомянутые этапы процесса интеграции данных. Рассмотрены также примеры аналитических запросов на языке HiveQL над единой схемой хранилища, которые могут быть использованы для планирования ПСО.

Извлечение структурированных данных из текстовых документов

При работе с неструктурированными текстовыми данными нужно сначала извлечь из них необходимую структурированную информацию.

Для извлечения информации о чрезвычайных ситуациях в Арктической зоне из сообщений из социальных сетей (Twitter и Facebook) предложены и реализованы методы в работах [14, 15]. Описаны методы сбора сообщений о чрезвычайных ситуациях, а также извлечения информации из текстов, включая названия географических объектов, наименования морских и речных судов, имена персон, названия организаций, факты чрезвычайной ситуации. Предложенная система сбора сообщений и извлечения из них структурированной информации включена в общую архитектуру системы извлечения информации из данных по Арктической зоне [2] в качестве подсистемы интеллектуального анализа текстов.

Для иллюстрации работы подсистемы анализа текстов из социальных сетей рассмотрим в качестве примера следующее сообщение в Twitter:

```
Chinese seismic vessel aimed for Russian #Barents Sea oil at logistics port #Kirkenes
```

Из этого сообщения система извлекает географические объекты «Barents Sea», «Kirkenes». Результат представляется в формате JSON:

```
[{
    "id": {
```

```
        "coll_id": "8002"
        , "res_id": {
            "site_id": "9b290c9f3bdaa68c"
            , "doc_id": "3649a5559a62"
        }
    }
    , "entities": [
      {
        "token": "Barents Sea",
        "tag": "I-ALOC",
        "end": 53,
        "begin": 42
      },
      {
        "token": "Kirkenes",
        "tag": "I-ALOC",
        "end": 85,
        "begin": 77
      }
    ]
}]
```

При этом слот *id* отвечает составному идентификатору сообщения, а слот *entities* – сущностям, извлеченным из сообщения. Указывается тип сущности (*tag*) и положение сущности в тексте сообщения (*begin, end*).

Также извлекать информацию из текстов можно, применив правила извлечения на основе регулярных выражений. В качестве примера рассмотрим извлечения информации из почтовых сообщений от системы КОСПАС-САРСАТ с использованием языка разработки экстракторов для текстовой аналитики AQL [16], поставляемого в составе решения IBM BigInsights Text Analytics.

Рассмотрим пример поступающего сообщения от системы КОСПАС-САРСАТ (здесь приведена лишь часть сообщения):

```
DATE: 06 APR 14 0832Z
FROM: MCC RUSSIA
TO : RCC RUSSIA
FORMAT FILE: RCC406M.FMT
1. DISTRESS COSPAS-SARSAT POSITION RESOLVED ALERT
2. MSG NO: 44032 CMC REF: 2226283082FFBFF
3. DETECTED AT: 06 APR 14 0827 UTC BY SARSAT S11
...
8. POSITIONS:
           RESOLVED - 44 53.8 S 039 44.0 W
           DOPPLER A - 44 53.8 S 039 44.0 W
```

Следующая программа на языке AQL позволяет извлекать необходимые данные (такие как дата отправления сообщения *SentDate*, дата обнаружения *DetectionDate*, идентификатор сообщения *MessageId*, долгота *Longitude*, широта *Latitude*) из текстовых сообщений на основе регулярных выражений с использованием оператора создания представления (взгляда) *create view*:

```
create view SentDate as
    extract regex /DATE: ([\w ]*)/ on D.text return
        group 1 as text
    from Document D;
create view DetectionDate as
    extract regex /3. DETECTED AT: (\d* \w* \d* \d*) UTC/
            on D.text return
```

```
        group 1 as text
    from Document D;
create view MessageId as
    extract regex /2. MSG NO: (\d*)/ on D.text return
        group 1 as text
    from Document D;
create view LongLat as
    extract regex /(\d* \d*.\d*) [NS] (\d* \d*.\d*) [WE]/
            on p.longlat return
        group 1 as longitude
        and group 2 as latitude
    from Positions2 p;
```

Результат применения этих правил представляется в табличном виде в формате CSV:

```
"05 APR 14 0833Z","05 APR 14 0826","44019","00 00.0","000 00.0"
"06 APR 14 0815Z","06 APR 14 0814","44030","00 00.0","000 00.0"
"06 APR 14 0832Z","06 APR 14 0827","44032","44 53.8","039 44.0"
```

Загрузка файлов и приведение данных к единому формату

Загрузка файлов, извлеченных из источников данных, в файловую систему HDFS осуществляется с помощью команды *hadoop fs -put* системы Hadoop.

Данные из исходных коллекций могут представляться в разных форматах (например, CSV, XML). Для применения методов интеграции все данные необходимо привести к единому формату, в качестве которого выбран JSON [13]. Приведение осуществляется с использованием языка Jaql [17]. Например, данные из СМС «Виктория», содержащие основные данные о корабле (название, страну, позывной, номер ИМО) и данные о движении корабля (текущие координаты, время, курс), представленные а формате XML, приводятся к JSON следующим образом:

```
vd = read(lines("/arctic/input/victoria.xml"));
vdj = vd -> strJoin("") -> xmlToJson() -> toArray();
vdj = vdj."ShipPositionResponse"."shipPositions"
-> expand
-> transform {
    uid: $.id, $."callSign", $."countryId", $."course", $."id", $."imo",
    $."isoCountryCode", $."latitude", $."longitude", $."marineReg",
    $."mmsi", $."name", $."nameLat", $."receiveDate", $."shipTypeId",
    $."source", $."sourceId", $."speed"};
vdj->write(jsonText("hdfs:/arctic/input/ShipPosition.json"));
```

Непосредственное преобразование из XML в JSON выполняется с использованием функции *xmlToJson*. При помощи операций *expand* и *transform* производится упрощение структуры для приведения к виду, пригодному для дальнейшей трансформации средствами языка HIL [18]. Пример результирующего документа выглядит следующим образом:

```
[{
  "callSign": "UCSZ", "countryId": "341", "course": "79", "id": "7286",
  "imo": "9344875", "isoCountryCode": "643", "latitude": "59.67478",
  "longitude": "28.4084835", "marineReg": "040188", "mmsi": "273310710",
  "name": "АСКОЛЬД", "nameLat": "ASKOLD",
  "receiveDate": "2017-01-11T15:20:11Z", "shipTypeId": "107",
  "source": "TRANSAS", "sourceId": "3", "speed": "0", "uid": "7286"
}]
```

Преобразование данных к схеме хранилища

Таблица. ***Соответствия элементов схемы СМС «Виктория» и схемы хранилища***

Схема хранилища	Схема источника
Отношение Vehicle	Элемент ShipPosition
Call	callSign
Name	Name
latName	nameLat
Country	isoCountryCode
Отношение Vessel	Элемент ShipPosition
imoNumber	Imo
mmsi	mmsi
Отношение Point	Элемент ShipPosition
latitude	latitude
longitude	longitude
Отношение TrackPoint	Элемент ShipPosition
course	course
hSpeed	speed
pointTime	receiveDate

Для каждого источника данных устанавливается соответствие между элементами его схемы и элементами схемы хранилища, используемое для преобразования данных, заданных в исходной схеме, в данные, представляемые в целевой схеме.

Рассмотрим установленные соответствия для схемы данных СМС «Виктория». Атрибуты элемента *ShipPosition* исходной схемы СМС «Виктория» соответствуют атрибутам четырех отношений целевой схемы: *Vessel*, *Vehicle*, *Point* и *TrackPoint* [4]. В таблице приведены соответствия между атрибутами для каждого отношения.

Более подробно соответствия элементов схем хранилища и источников рассмотрены в работе [2]. Фактически, соответствия элементов схем задают правила преобразования данных из схемы источника к схеме хранилища.

В качестве языка реализации правил преобразования данных в работе используется декларативный язык HIL [18], разработанный компанией IBM и ориентированный на решение задач преобразования данных, отождествления различных сущностей, соответствующих одному объекту реального мира, и слиянию таких сущностей в единую интегрированную сущность. Программа на языке HIL компилируется в программу на языке Jaql, которая, в свою очередь, запускается на платформе Hadoop. Это позволяет автоматически масштабировать процесс преобразования больших объемов данных.

Правило преобразования данных на языке HIL в общем виде выглядит следующим образом:

```
insert into TargetEntity
select [
    target_attr1: s.source_attr,
    target_attr2: function_transform(s),
    target_attr3: constant,
    ...
    ]
from SourceEntity s;
```

Здесь *SourceEntity* – элемент исходной коллекции; *TargetEntity* – элемент схемы хранилища (целевой элемент); *target_attr* – атрибуты элемента *TargetEntity*; *source_attr* – атрибут элемента *SourceEntity*; *transform_function* – функция преобразования атрибутов элемента *SourceEntity*; *constant* – числовая или строковая константа. Выражения преобразования атрибутов формируются на основе установленных соответствий между элементами схем. *TargetEntity* также можно считать коллекцией, формируемой в результате применения правила. Структура сущностей коллекции (набор атрибутов) определяется в секции *select*.

Приведем пример фрагмента программы преобразования элемента *ShipPosition* исходной схемы СМС «Виктория» в элементы целевой схемы:

```
// Исходная схема
declare ShipPositions : ?;

// Целевая схема
declare VehicleVICT : ?;
```

```
declare VesselVICT : ?;
...

// Функции разрешения конфликтов
declare get_country: function string to string;
declare get_vehicle_id: function string to string;
declare get_vessel_id: function string to string;
...

// Правила преобразования
insert into VehicleVICT
select [
    uid: get_vehicle_id(sp.uid)
    , call: sp.callSign
    , name: sp.name
    , latName: sp.nameLat
    , country: get_country(sp.isoCountryCode)
    , vehicleSubtype: "Vessel"
    ]
from ShipPositions sp;

insert into VesselVICT
select [
    uid: get_vessel_id(sp.uid)
    , imoNumber: sp.imo
    , mmsi: sp.mmsi
    , vehicleId: get_vehicle_id(sp.uid)
    ]
from ShipPositions sp;
```

Как показано выше, элемент исходной коллекции *ShipPositions* содержит данные, соответствующие четырем отношениям схемы хранилища: *Vessel*, *Vehicle*, *Point*, *TrackPoint*. Для экономии места в примере продемонстрировано преобразование только в два отношения.

Подобные правила трансформации создаются для всех интегрируемых источников. Одному отношению схемы хранилища могут соответствовать элементы из разных источников. Например, метаданные о судах из системы ЕСИМО также соответствуют отношениям *Vessel*, *Vehicle*. Для уникальной идентификации целевых элементов, полученных из различных источников, в правилах слияния данных (рассматриваемых в следующем разделе) к названиям целевых элементов добавляется уникальный суффикс. В рассматриваемом примере к названиям элементов добавляется суффикс *VICT*: *VehicleVICT* и *VesselVICT*.

Каждый целевой элемент содержит атрибут *uid*, значение которого формируется с помощью функций, порождающих уникальные идентификаторы. Эти атрибуты являются, фактически, первичными ключами. Атрибут *vehicleSubtype* в элементе *VehicleVICT* является служебным и служит для реализации отношения тип-подтип. Функция *get_country(sp.isoCountryCode)* является примером функции разрешения конфликтов между исходной и целевой схемами. В данном примере в исходной коллекции данные о стране представлены в виде ISO-кода страны, а в целевой схеме данные представляются в виде названия страны. Функция *get_country(sp.isoCountryCode)* реализует это преобразование из ISO-кода в название страны.

В результате применения программы преобразования формируются данные в виде четырех файлов: *VehicleVICT.json*, *VesselVICT.json*, *PointVICT.json*, *TrackPointVICT.json*. Каждый файл соответствует отношению целевой схемы и содержит кортежи этого отношения в формате JSON. Приведем фрагмент примера преобразованных данных для СМС «Виктория»:

```
// Vehicle.json
```

```
[{
  "call": "UCSZ",
  "country": "Russia",
  "latName": "ASKOLD",
  "name": "АСКОЛЬД",
  "uid": "7286_01",
  "vehicleType": "Vessel"
}]

// Vessel.json
[{
  "imoNumber": "9344875",
  "mmsi": "273310710",
  "uid": "7286_02",
  "vehicleId": "7286_01"
}]
```

Слияние данных из разных источников

Часто разные источники содержат данные об одних и тех же объектах реального мира. При этом возникает задача поиска одинаковых сущностей и слияния данных из этих одинаковых сущностей в единую интегрированную сущность. Создание такой интегрированной сущности позволяет упростить анализ данных. В качестве языка реализации правил отождествления различных сущностей и их слияния в рассматриваемой системе используется язык HIL [18].

Программы отождествления различных сущностей на языке HIL основываются на использовании оператора разрешения сущностей (entity resolution) *create link*:

```
create link TargetEntityLink as
select [
    sourceEntity1: [ <attribute_list> ],
    sourceEntity2: [ <attribute_list> ]
    ]
from SourceEntity1 s1, SourceEntity2 s2
match using
    rule1: <matching_rule>,
    ...
    ruleN: <matching_rule>;
```

Здесь *SourceEntity1* и *SourceEntity2* – исходные элементы; *TargetEntityLink* – вспомогательный элемент, содержащий данные о найденных одинаковых сущностях. Элемент *TargetEntityLink* содержит два атрибута, каждый из которых, в свою очередь, содержит данные (<*attribute_list*>) из соответствующих исходных элементов. Отождествление сущностей из разных источников, соответствующих одному объекту реального мира, осуществляется на основе правил сопоставления (<*matching_rule*>). В результате выполнения этой программы *TargetEntityLink* будет содержать информацию о том, какие конкретно из правил сработали для отождествления сущностей (атрибут *ruleFired*), и общее число сработавших правил (атрибут *rulescount*).

Приведем пример программы отождествления сущностей элементов *VehicleVICT* и *VehicleESIM*, полученных на этапе преобразования данных (см. предыдущий раздел) для коллекции СМС «Виктория» и коллекции метаданных о судах из системы ЕСИМО:

```
// Transformation rules
create link VehicleLink as
select [
    vehicleVict: [uid: vv.uid, call: vv.call, name: vv.name],
    vehicleEsim: [uid: ve.uid, call: ve.call, name: ve.name] ]
```

```
from VehicleVICT vv, VehicleESIM ve
match using
    rule1: vv.call = ve.call;
```

Отождествление сущностей происходит по значению атрибута *call* – позывному судна. Полученные в результате выполнения этой программы сущности элемента *VehicleLink* представляются в формате JSON следующим образом:

```
[{
  "ruleFired": "rule1",
  "rulescount": 1,
  "vehicleEsim": {"call": "UCSZ", "name": "ASKOLD", "uid": "4_01"},
  "vehicleVict": {"call": "UCSZ", "name": "АСКОЛЬД", "uid": "7286_01"}
}]
```

Программа слияния отождествленных сущностей на языке HIL основывается на использовании оператора *insert into*:

```
insert into TargetEntity
select [
    <target_attr1>: <attribute_expression>
    ...
    , <target_attrN>:<attribute_expression>
    ]
from SourceEntity1 s1, SourceEntity1 s1, SourceLink sl;
where <where_clause>
```

Здесь *TargetEntity* – целевой элемент; *SourceEntity1* и *SourceEntity2* – исходные элементы; *SourceEntityLink* – вспомогательный элемент, содержащий данные о найденных одинаковых сущностях элементов *SourceEntity1* и *SourceEntity2*; *<target_attr>* – атрибуты элемента *TargetEntity*; *<attribute_expression>* – выражения порождения целевых атрибутов из атрибутов исходных элементов (при этом можно использовать функции, реализующие стратегии слияния значений атрибутов, например, выбирать максимальное значение или производить конкатенацию строк-значений одинаковых атрибутов исходных элементов); выражение *<where_clause>* задает условия на слияние сущностей элементов *SourceEntity1* и *SourceEntity2*.

Приведем пример программы слияния сущностей для элементов целевой схемы *Vehicle* и *Vessel* из элементов *VehicleVICT* и *VehicleESIM*, *VesselVICT* и *VesselESIM* (полученных на этапе преобразования данных для коллекции СМС «Виктория» и коллекции метаданных о судах из системы ЕСИМО) соответственно с помощью ранее созданного элемента *VehicleLink*:

```
insert into Vehicle
select [
    uid: get_vehicle_id(vv.uid, ve.uid)
    , call: vv.call
    , name: vv.name
    , latName: vv.latName
    , country: vv.country
    , vehicleType: vv.vehicleType
    , description: ve.description
    , maxCrew: ve.maxCrew
    , maxRange: ve.maxRange
    , maxSpeed: ve.maxSpeed
    , ownerId: ve.ownerId
    , vehicleSubtype: vv.vehicleSubtype
    ]
```

```
from VehicleVICT vv, VehicleESIM ve, VehicleLink vl
where vv.uid = vl.vehicleVict.uid and ve.uid = vl.vehicleEsim.uid;

insert into Vessel
select [
    uid: get_vessel_id(vv.uid, ve.uid)
    , imoNumber: vv.imoNumber
    , mmsi: vv.mmsi
    , vehicleId: get_vehicle_id(vv.vehicleId, ve.vehicleId)
    , length: ve.length
    , width: ve.width
    , deadweight: ve.deadweight
    , displacement: ve.displacement
    ]
from VesselVICT vv, VesselESIM ve, VehicleLink vl
where vv.vehicleId = vl.vehicleVict.uid and
      ve.vehicleId = vl.vehicleEsim.uid;
```

Здесь *get_vehicle_id* и *get_vessel_id* – функции генерации уникального ключа на основе ключей исходных сущностей. Для атрибутов *call*, *name*, *country* и *vehicleSubtype*, которые есть и в элементе *VehicleVICT*, и в элементе *VehicleESIM*, была реализована стратегия выбора значений из элемента *VehicleVICT*.

Приведем пример результата слияния данных из СМС «Виктория» и системы ЕСИМО. Результатом являются сущности из коллекций *Vehicle* и *Vessel*:

```
// Vehicle.json
[{
  "call": "UCSZ",
  "country": "Russia",
  "description": "",
  "latName": "ASKOLD",
  "maxCrew": "",
  "maxRange": "",
  "maxSpeed": "10.4",
  "name": "АСКОЛЬД",
  "ownerId": "4_03",
  "uid": "7286_01_4_01",
  "vehicleType": "Vessel"
}]

// Vessel.json
[{
  "deadweight": "184",
  "displacement": "498",
  "imoNumber": "9344875",
  "length": "36.65",
  "mmsi": "273310710",
  "uid": "7286_02_4_02",
  "vehicleId": "7286_01_4_01",
  "width": "12.82"
}]
```

Верификация программ интеграции данных

Идея подхода к верификации программ интеграции данных, предложенного и программно реализованного в [7], состоит в том, чтобы сообщить программам интеграции данных семантику в языке специфи-

каций (AMN [19]), поддержанном средствами формального автоматического и/или интерактивного доказательства (Atelier B [20]): для языка интеграции данных (HIL) строится его отображение в язык спецификаций. Свойства программ, подлежащие проверке, представляются в виде выражений выбранного языка спецификаций. Затем с использованием формальных средств доказательства спецификация, выражающая семантику конкретного потока работ интеграции данных, проверяется на соответствие необходимым свойствам.

Продемонстрируем применение подхода для верификации программ интеграции, приведенных в качестве примеров в предыдущих разделах. Совокупность правил на языке HIL, отвечающих преобразованию и слиянию данных о судах из СМС «Виктория» и ЕСИМО, формализуется в языке AMN следующим образом (приведен фрагмент спецификации):

```
REFINEMENT ArcticRef
VARIABLES state, VesselVICT, VesselESIM, Vessel, VehicleLink, ...

INVARIANT
Vessel: POW(struct(uid: STRING_TYPE, imoNumber: STRING_TYPE,
  mmsi: STRING_TYPE, vehicleId: STRING_TYPE, length: STRING_TYPE,
  width: STRING_TYPE, deadweight: STRING_TYPE,
  displacement: STRING_TYPE)) &
state : struct(
  VehicleLinkCreated: BOOL,
  VehicleESIMFromShipInserted: BOOL,
  VesselESIMFromShipInserted: BOOL,
  VehicleVICTFromShipPositionsInserted: BOOL,
  VesselVICTFromShipPositionsInserted: BOOL,
  VehicleFromVehicleVICTVehicleESIMVehicleLinkInserted: BOOL,
  VesselFromVesselVICTVesselESIMVehicleLinkInserted: BOOL)

INITIALISATION
  VesselVICT := {} || VesselESIM := {} || Vessel := {} ||
  VehicleLink := {} || ... ||
  state := rec(VehicleLinkCreated: FALSE,
    VehicleESIMFromShipInserted: FALSE,
    VesselESIMFromShipInserted: FALSE,
    VehicleVICTFromShipPositionsInserted: FALSE,
    VesselVICTFromShipPositionsInserted: FALSE,
    VehicleFromVehicleVICTVehicleESIMVehicleLinkInserted: FALSE,
    VesselFromVesselVICTVesselESIMVehicleLinkInserted: FALSE)

OPERATIONS
insertIntoVesselFromVesselVICTVesselESIMVehicleLink =
SELECT
  state'VesselESIMFromShipInserted = TRUE &
  state'VehicleLinkCreated = TRUE &
  state'VesselVICTFromShipPositionsInserted = TRUE
THEN
  Vessel := (Vessel \/ {rr | #(vv, ve, vl).(vv : VesselVICT &
    ve : VesselESIM & vl : VehicleLink &
    rr = rec(uid: get_vessel_id(vv'uid, ve'uid), imoNumber: vv'imoNumber,
      mmsi: vv'mmsi,
      vehicleId: get_vehicle_id(vv'vehicleId, ve'vehicleId),
      length: ve'length, width: ve'width, deadweight: ve'deadweight,
      displacement: ve'displacement) &
      vv'vehicleId = vl'vehicleVict'uid &
      ve'vehicleId = vl'vehicleEsim'uid)});
```

```
  state'VesselFromVesselVICTVesselESIMVehicleLinkInserted := TRUE
END
```

Семантическая спецификация *ArcticRef* относится к виду REFINEMENT (уточнение). Каждой из исходных, целевых, вспомогательных коллекций данных соответствует переменная в секции VARIABLES (например, *Vessel*). Кроме того, присутствует переменная *state*, определяющая порядок исполнения отдельных операций преобразования и интеграции. В секции INVARIANT переменные типизируются, в секции INITIALISATION – инициализируются. Каждому правилу языка HIL соответствует операция спецификации (секция OPERATIONS). В примере приведена лишь одна операция, соответствующая правилу формирования коллекции *Vessel*. Принципы и детали отображения подробно объяснены в [7].

В качестве свойства программы интеграции, подлежащего верификации, рассматривается сохранение информации о судах при интеграции, выражаемое следующей формулой:

```
state'VehicleFromVehicleVICTVehicleESIMVehicleLinkInserted = TRUE &
state'VesselFromVesselVICTVesselESIMVehicleLinkInserted= TRUE =>
  !(pp, ss).(pp: ShipPositions & ss: Ship & pp'callSign = ss'call_sign =>
    #(vh, vs).(vh: Vehicle & vs: Vessel & vh'call = pp'callSign &
      vs'vehicleId = vh'uid & vs'mmsi = pp'mmsi &
      vs'deadweight = ss'deadweight )
```

В формуле утверждается, что для любой пары сущностей из исходных коллекций *ShipPositions* и *Ship* соответственно с совпадающим позывным (*callSign*, *call_sign*) по завершении процесса интеграции в результирующих коллекциях *Vehicle* и *Vessel* присутствуют сущности, значения позывного (*call*) и других существенных атрибутов (например, *mmsi*, *deadweight*) которых совпадают со значениями соответствующих атрибутов исходных сущностей. Эта формула добавляется в инвариант семантической спецификации, после чего спецификация загружается в программное средство Atelier B и ее корректность доказывается с использованием средств автоматического и интерактивного доказательства.

Реализация хранилища и загрузка интегрированных данных в хранилище

Реализация хранилища средствами СУБД Hive. Схема хранилища информации по Арктической зоне (целевая схема) реализована в виде базы данных Hive на основе файлового хранилища HDFS. Для каждой сущности целевой схемы создается таблица в Hive. В соответствии с типами сущностей целевой схемы [4] созданы 43 таблицы с атрибутами, соответствующими атрибутам типов.

Наследование, присутствующее в целевой схеме [4] для сокращения дублирования информации, моделируется средствами СУБД Hive следующим образом:

в таблице, соответствующей родовому типу, определяется атрибут уникального идентификатора объекта и атрибут с фиксированным числом значений, определяющих, какому подтипу родового типа принадлежит данная сущность;

в таблицах, соответствующих подтипам объектов, определяется атрибут для ссылки на уникальный идентификатор объекта и создания отдельных уникальных идентификаторов для таблицы подтипа, данный атрибут однозначно идентифицирует экземпляр сущности (к тому же СУБД Hive не предоставляет контроля внешних ссылок и ключей);

для подтипов, которые не несут в себе дополнительной информации относительно родового типа (не содержат собственных атрибутов), отдельные таблицы не создаются, однако в специализированном атрибуте родового типа указывается значение, говорящее о типе объекта.

Рассмотрим создание таблиц Hive на примере некоторых сущностей предметной области. Таблица *Vehicle* описывает сущности, являющиеся транспортными средствами, такие как объекты поиска или средства поиска в поисковых операциях.

```
CREATE TABLE Vehicle (
    vehicleId string,
```

```
    vehicleSubtype string,
    vehicleType string,
    name string,
    latName string,
    call string,
    boardNumber string,
    operation string,
    incident string,
    ...
);
```

Таблица *Vehicle* реализует родовой тип для различных типов объектов (самолетов и вертолетов, судов, наземного транспорта) и содержит общие для всех типов транспортных средств атрибуты: наименование и идентификацию объектов (*name*, *latName*, *call*, *boardNumber*), их разновидности (*vehicleType*), связь с ПСО (*operation*, *incident*), а также принадлежность, различные характеристики, состояние, описание оснащения.

Для реализации уникальной идентификации, внешних ссылок и наследования между сущностями вводятся следующие атрибуты: *vehicleId* – уникальный идентификатор объекта, используемый как в родовом типе, так и в подтипах; *vehicleSubtype* – наименование подтипа сущности, одноименное с именем соответствующей таблицы.

Для подтипов объектов, являющихся транспортными средствами, в целевой схеме определены разные таблицы, для которых таблица *Vehicle* является таблицей родового типа. В частности, описание морских и речных судов как транспортных средств реализовано таблицей *Vessel*:

```
CREATE TABLE Vessel (
    vehicleId string,
    imoNumber string,
    pmpcNumber string,
    mmsi string,
    boardColor string,
    deckColor string,
    ...
);
```

Таблица *Vessel*, в дополнение к таблице *Vehicle*, также используемой при описании морских и речных судов, определяет собственные атрибуты, в том числе идентификаторы судов в разных форматах (*imoNumber*, *pmpcNumber*, *mmsi*), отличительные признаки (*boardColor*, *deckColor*) и другие дополнительные характеристики судов.

Для реализации подтипа сущности *Vehicle* таблица *Vessel* содержит атрибут *vehicleId*, являющийся, с одной стороны, внешней ссылкой на таблицу *Vehicle* по ее атрибуту *vehicleId*, а с другой стороны, уникальным идентификатором объекта, определяемым идентично как в родовом типе, так и в подтипе.

Структура информации о точках траекторий транспортных средств определяется таблицами *Point* и *TrackPoint*. Таблица *Point* реализует родовой тип точек с координатами (*latitude*, *longitude*), обеспечивающий возможность создания из них путей (*ordered*, *path*, *beginPointOf*, *endPointOf*) и связывания с транспортными средствами (*vehicle*) для задания маршрутов и отражения траекторий. Для точек, описывающих траектории и фактическое наблюдаемое положение объектов, используется подтип, реализуемый таблицей *TrackPoint*. Она включает в себя атрибуты времени (*pointTime*), высоты (*height*), скорости (*hSpeed*, *vSpeed*), курса (*course*) объекта. В обеих таблицах определяются атрибуты идентификатора объекта (*pointId*), а в таблице родового типа – атрибут, определяющий имя подтипа (*pointSubtype*):

```
CREATE TABLE Point (
    pointId string,
    pointSubtype int,
```

```
    latitude double,
    longitude double,
    ordered int,
    path string,
    beginPointOf string,
    endPointOf string,
    vehicle string
);

CREATE TABLE TrackPoint (
    pointId string,
    pointTime string,
    height double,
    hSpeed double,
    vSpeed double,
    course double
);
```

Информация о погодных условиях сохраняется в таблице *Weather*. Она содержит определение координат точки (*latitude*, *longitude*, *height*), время наблюдения (*observeTime*), ссылку на объект (*vehicle*), являющийся источником наблюдений, и набор наблюдений, включая температуру (*temperature*), ледовую ситуацию (*iceConcentration*), параметры ветра (*windDirection*, *windSpeed*) и другую информацию:

```
CREATE TABLE Weather (
    messageId string,
    latitude double,
    longitude double,
    observeTime string,
    height double,
    temperature double,
    windDirection string,
    windSpeed double,
    iceConcentration double,
    operation string,
    vehicle string
    ...
);
```

Таблица *SAROperation* связана с описанием ПСО. Она объединяет описание плана (*plan*), происшествия (*incident*), подчиненности (*country*, *coordCenter*), ссылки на координатора (*coordinator*), оператора (*recorder*) и другие сведения:

```
CREATE TABLE SAROperation (
    operationId string,
    country string,
    plan string,
    coordCenter string,
    coordinator string,
    recorder string,
    incident string,
    ...
);
```

Связи «один к одному» и «много к одному» реализуются атрибутами со ссылками на идентификаторы в целевых таблицах. Например, в таблице *SAROperation* атрибуты *coordCenter*, *coordinator*, *record-*

er, *incident* содержат ссылки на другие таблицы по идентификаторам. Специальные средства поддержки целостности внешних ссылок в языке HiveQL отсутствуют.

Инверсные связи «один к одному» и «один ко многим», присутствующие в схеме, на языке HiveQL не фиксируются, но реализованы с помощью определения представлений над таблицами Hive. В схеме определено 29 подобных представлений.

В частности, ссылка на операцию *operation* в сущности *Vehicle* в схеме имеет инверсную связь *searchObjects*, которая не реализуема атрибутом. Для ее реализации определено представление *SAROperation_searchObjects*. Данное представление производит соединение таблиц *SAROperation* и *Vehicle* по идентификатору операции:

```
CREATE VIEW SAROperation_searchObjects (operationId, searchObjects) AS
SELECT DISTINCT SAROperation.operationId, Vehicle.vehicleId
FROM SAROperation JOIN Vehicle
ON SAROperation.operationId = Vehicle.operation;
```

Связи «много ко многим» потребовали создания специальных таблиц. Так, с несколькими транспортными средствами может быть связан маршрут. При этом с одним транспортным средством может быть связан набор маршрутов. Поэтому для реализации такой связи создается таблица с парой атрибутов, хранящих ссылки на идентификаторы *vehicleId* и *pathId*:

```
CREATE TABLE VehicleRoute (
    vehicles string,
    routes string
);
```

Средства загрузки данных в хранилище Hive. В результате преобразования данных из определенного источника в целевую схему образуется набор файлов в формате JSON с именами, совпадающими с названиями сущностей целевой схемы. Соответственно, данные из этих файлов должны быть загружены в одноименные таблицы Hive в соответствии с их структурой.

Перед началом загрузки данных необходима предварительная коррекция JSON-файлов, созданных в процессе преобразования данных источников к целевой схеме хранилища. Из-за особенностей средств работы с JSON в Hive эти файлы должны содержать по одной структурированной записи JSON на одну строку. Поэтому необходимо произвести следующие действия: удаление символов коллекции «[» и «]» в начале и в конце файлов; замену переводов строк внутри структуры на пробелы; замену запятых, являющихся разделителями записей, на переводы строк.

Например, для файла *Vehicle.json* это можно сделать с помощью следующей инструкции в Unix-подобных системах:

```
cat Vehicle.json | tr "\n" " " | sed "s/},{/}\n{/g" | sed "s/\[{/{/g"
    | sed "s/}\]/}/g" > Vehicle.json
```

Дальнейшая работа производится в среде Hive на языке HiveQL. Для загрузки данных из интегрированных источников используются функции работы с форматом JSON, присутствующие в Hive.

Рассмотрим процесс загрузки данных на примере таблицы *Vehicle*, соответствующей родовому типу для сущностей, описывающих транспортные средства разных типов.

Вначале создается временная таблица *JsonVehicle*, в значения единственного атрибута которой записываются строки с загружаемыми данными из файла *Vehicle.json*, рассматриваемого как текстовый файл:

```
DROP TABLE IF EXISTS JsonVehicle;
CREATE TEMPORARY TABLE JsonVehicle(json string);
LOAD DATA LOCAL INPATH 'Vehicle.json' INTO TABLE JsonVehicle;
```

Затем запросом к временной таблице *JsonVehicle* с помощью функции *json_tuple* разбираются строки JSON, формируется представление с набором атрибутов, соответствующим структуре таблицы *Vehicle*, и производится вставка результата запроса в таблицу *Vehicle*. Запрос содержит все атрибуты таблицы целевой схемы и не зависит от того, из каких источников преобразуются и загружаются данные и какие атрибуты они содержат. Атрибутам, отсутствующим в загружаемых данных, будет присвоено значение *NULL*. В завершение временная таблица *JsonVehicle* удаляется.

```
INSERT INTO TABLE Vehicle (
    vehicleId, vehicleSubtype, vehicleType, name, latName, call,
    boardNumber, country, fuelLoad, fuelMax, maxSpeed, maxRange,
    peopleOnBoard, maxCrew, equipment, description, owner, operator,
    operation, incident, unit)
SELECT v.vehicleId, v.vehicleSubtype, v.vehicleType, v.name, v.latName,
    v.call, v.boardNumber, v.country, v.fuelLoad, v.fuelMax, v.maxSpeed,
    v.maxRange, v.peopleOnBoard, v.maxCrew, v.equipment,                  v.description,
    v.owner, v.operator, v.operation, v.incident, v.unit
FROM JsonVehicle
LATERAL VIEW json_tuple(JsonVehicle.json,
    'uid', 'vehicleSubtype', 'vehicleType', 'name', 'latName', 'call',
    'boardNumber', 'country', 'fuelLoad', 'fuelMax', 'maxSpeed',
    'maxRange', 'peopleOnBoard', 'maxCrew', 'equipment', 'description',
    'owner', 'operator', 'operation', 'incident', 'unit') v
AS    vehicleId, vehicleSubtype, vehicleType, name, latName, call,
    boardNumber, country, fuelLoad, fuelMax, maxSpeed, maxRange,
    peopleOnBoard, maxCrew, equipment, description, owner, operator,
    operation, incident, unit;
DROP TABLE JsonVehicle;
```

Одним из подтипов сущности *Vehicle* является сущность *Vessel*, описывающая речные и морские суда. На его примере рассмотрим загрузку таблиц, соответствующих подтипам. Загрузка производится отдельно из файла *Vessel.json*, также адаптированного к средствам загрузки данных в формате JSON в СУБД Hive:

```
cat Vessel.json | tr "\n" " " | sed "s/},{/}\n{/g" | sed "s/\[{/{/g" | sed "s/}\]/}/g"
> Vessel.json
```

В среде Hive аналогично с помощью функции *json_tuple* производится выявление всех атрибутов таблицы *Vessel*, включая внешнюю ссылку *vehicleId* на таблицу *Vehicle* в качестве реализации наследования. Данный атрибут также может служить уникальным идентификатором записей таблицы *Vessel*.

```
CREATE TEMPORARY TABLE JsonVessel(json string);
LOAD DATA LOCAL INPATH 'Vessel.json' INTO TABLE JsonVessel;
INSERT INTO TABLE Vessel (
    vehicleId, imoNumber, pmpcNumber, mmsi, boardColor, deckColor,
    length, width, mouldedDepth, displacement, deadweight, draught)
SELECT v.vehicleId, v.imoNumber, v.pmpcNumber, v.mmsi, v.boardColor,
    v.deckColor, v.length, v.width, v.mouldedDepth, v.displacement,
    v.deadweight, v.draught
FROM JsonVessel
LATERAL VIEW json_tuple(JsonVessel.json,
    'vehicleId', 'imoNumber', 'pmpcNumber', 'mmsi', 'boardColor',
    'deckColor', 'length', 'width', 'mouldedDepth', 'displacement',
    'deadweight', 'draught') v
AS    vehicleId, imoNumber, pmpcNumber, mmsi, boardColor, deckColor,
    length, width, mouldedDepth, displacement, deadweight, draught;
```

```
DROP TABLE JsonVessel;
```

Подобная процедура загрузки данных в хранилище Hive производится для каждой из сущностей, если файлы с соответствующим именем в формате JSON присутствуют. Несмотря на раздельную загрузку каждой из сущностей, данные из разных таблиц связаны друг с другом за счет того, что необходимые идентификаторы и ссылки по ним были сгенерированы уже на этапе интеграции источников и преобразования данных к целевой схеме.

Анализ информации в хранилище Hive

Над консолидированным распределенным хранилищем информации из разных источников производится анализ данных. Обработка данных, относящихся к сущностям, реализованным с использованием наследования, производится с помощью операций соединения между таблицами родового типа и подтипа по идентификаторам объектов. При работе с конкретным экземпляром сущности обращение за значениями его атрибутов производится посредством выборки данных из таблицы родового типа и таблицы подтипа, если она создана.

Рассмотрим некоторые запросы на языке HiveQL [5] для решения задач над хранилищем Hive.

З а д а ч а 1 . Выяснить данные о погодных условиях, включая температуру и ледовую ситуацию, в районе известного местонахождения объекта поиска данной поисковой операции на данный момент.

Для решения этой задачи необходимо выяснить, какие транспортные средства являются объектами поиска в данной операции (идентификатор передается в переменной *operationId*) и имеют известные траектории:

```
SELECT p.vehicle as searchObject, max(t.pointTime) as time
FROM Point p
JOIN TrackPoint t ON p.pointId = t.pointId
JOIN SAROperation_searchObjects so ON p.vehicle = so.searchObjects
WHERE operationId like "${hiveconf: operationId}"
GROUP BY p.vehicle;
```

Данный запрос обладает следующими особенностями:

соединяет таблицу точек траекторий *TrackPoint* с родовой таблицей *Point* для одновременного использования атрибутов времени *pointTime* и наблюдаемого объекта *vehicle*;

использует представление *SAROperation_searchObjects*, реализующее связь *searchObjects* в сущности *SAROperation* для связи с текущей поисковой операцией;

накладывает ограничение на идентификатор операции *operationId*;

возвращает таблицу объектов поиска и последних дат их наблюдения.

Пример результата запроса выглядит следующим образом:

```
searchObject    time
2231252_01      2017-01-11T15:20:11Z
```

Затем необходимо выяснить положение выбранного объекта (его идентификатор передается в переменной *searchObject*) по последней известной дате (*time*):

```
SELECT p.latitude as latitude, p.longitude as longitude
FROM Point p
JOIN TrackPoint t ON p.pointId = t.pointId
WHERE p.vehicle like "${hiveconf: searchObject}"
    AND t.pointTime like "${hiveconf: time}";
```

Запрос соединяет таблицы *Point* и *PointTrack*, накладывает ограничение по объекту поиска и времени и возвращает координаты объекта. Пример результата запроса выглядит следующим образом:

```
latitude    longitude
59.87319    30.2163658
```

Наконец, нужно найти данные о погоде на необходимую дату (*time*), например, в радиусе одного градуса от точки нахождения объекта. Координаты передаются через переменные *latitude* и *longitude*.

```
SELECT temperature, windspeed, iceConcentration
FROM Weather
WHERE SQRT(POW(${hiveconf:latitude} - latitude, 2) +
           POW(${hiveconf:longitude} - longitude, 2)) < 1.0
        AND observeTime contains "${hiveconf: time}";
```

Для передаваемых координат вычисляется ограничивающая окрестность для точек замера погодных условий из таблицы *Weather*, также ограничивается необходимая дата. В результате ответ на запрос содержит искомые характеристики погодных условий:

```
temperature    windSpeed    iceConcentration
13.0           7.0          0.0
```

З а д а ч а 2 . Найти известные траектории перемещения судов – объектов поиска, связанных с операцией с определенным наименованием.

Этого можно добиться одним запросом:

```
SELECT h.vehicleId as vehicleId, s.imoNumber as imoNumber,
       p.latitude as latitude, p.longitude as longitude,
       t.pointTime as time
FROM SAROperation op
JOIN Vehicle h ON h.operation = op.operationId
JOIN Vessel s ON h.vehicleId = s.vehicleId
JOIN Point p ON p.vehicle = h.vehicleId
JOIN TrackPoint t ON p.pointId = t.pointId
WHERE (h.vehicleSubtype like "Vessel")
       AND (p.pointSubtype like "TrackPoint")
       AND (op.name like "${hiveconf:operationName}")
ORDER BY t.pointTime;
```

Запрос содержит:

соединение таблиц *Vehicle* и *Vessel* по идентификатору *vehicleId* для реализации наследования атрибутов супертипа *Vehicle*, при этом выносится условие, что значение атрибута *vehicleSubtype* равно «*Vessel*»;

соединение таблиц *Point* и *TrackPoint* по идентификатору *pointId* (для подобной же цели);

соединение таблиц *Vehicle* и *Point* по атрибутам *Vehicle.vehicleId* и *Point.vehicle*;

соединение результата с таблицей *SAROperation*;

выборку по операции с наименованием, передаваемым через переменную *operationName*;

возврат атрибутов *imoNumber*, *latitude*, *longitude*, *pointTime*, отсортированных по времени *pointTime*.

В результате исполнения запроса возвращается ответ, содержащий идентификаторы судов и траекторий их движения:

```
vehicleId    imoNumber    latitude    longitude    time
2231252_01   8717829      59.87319    30.2163658   2017-01-11T15:20:11Z
7286_01      9344875      59.67478    28.4084835   2017-01-11T15:20:11Z
7286_01      9344875      58.04583    28.2855402   2017-01-13T10:03:15Z
...
```

Для выполнения рассмотренных примеров запросов используется информация, собранная из различных информационных систем, интегрированная и сохраненная в однородной структуре в распределенном хранилище информации по Арктической зоне.

Таким образом, над хранилищем информации по Арктической зоне могут решаться сложные аналитические задачи посредством запросов в терминах единой схемы хранилища. Их формулирование не требует оперативного обращения к источникам данных, из которых уже собраны потенциально полезные данные, и нет необходимости в дополнительной разработке сложных распределенных процессов. При этом запросы могут привлекать одновременно данные различной природы, собранные из ряда не связанных друг с другом информационных систем и сохраненные в распределенном хранилище.

- Исследован подход к реализации методов интеграции данных по Арктической зоне в единое хранилище. В качестве конкретных источников данных, подлежащих интеграции, выбраны СМС «Виктория», комплексная интегрированная информационная система «МоРе», межведомственная информационная система ЕСИМО, международная спутниковая поисково-спасательная система КОСПАС-САРСАТ, программный комплекс «Поиск-Море». Рассмотрены и проиллюстрированы на примерах: извлечение структурированных данных из текстовых документов; приведение данных, полученных из источников, к единому формату; преобразование данных к схеме хранилища; слияние данных из разных источников для образования интегрированных представлений; верификация программ интеграции данных; особенности реализации хранилища; загрузка интегрированных данных в хранилище данных. Рассмотрены также примеры аналитических запросов на языке HiveQL над единой схемой хранилища, которые могут быть использованы для планирования ПСО.

Работа выполнена в рамках проекта РФФИ «Извлечение информации из разноструктурированных данных для решения задач информационной поддержки поисковых действий в арктической зоне» (грант №15-29-06045).

Литература

1. *Брюхов Д.О.* Источники данных для информационной поддержки поисково-спасательных операций // Системы высокой доступности. 2015. Т. 11. № 4. С. 83−89.
2. *Брюхов Д.О.*, *Скворцов Н.А.*, *Ступников С.А.* Методы интеграции разноструктурированных данных по Арктической зоне для извлечения информации, нацеленной на поддержку поисково-спасательных операций // Системы высокой доступности. 2017. Т. 13. № 2. С. 3−19.
3. *White T.* Hadoop: The Definitive Guide. Third Edition. O'Reilly Media. 2012.
4. *Скворцов Н.А.*, *Брюхов Д.О.* Разработка схемы хранилища данных для поддержки поисковых действий в Арктической зоне // Системы высокой доступности. 2017. Т. 13. № 2. С. 20−44.
5. *Capriolo E.*, *Wampler D.*, *Rutherglen J.* Programming Hive Data Warehouse and Query Language for Hadoop. O'Reilly Media. 2012.
6. *Miner D.* MapReduce Design Patterns: Building Effective Algorithms and Analytics for Hadoop and Other Systems. O'Reilly Media. 2012.
7. *Stupnikov S.* Semantics and Verification of Entity Resolution and Data Fusion Operations via Transformation into a Formal Notation // In: Data Analytics and Management in Data Intensive Domains. DAMDID/RCDL 2016. Communications in Computer and Information Science / Ed. by *L. Kalinichenko*, *S. Kuznetsov*, *Y. Manolopoulos*. Springer. 2017. V. 706. P. 145−162.
8. Система мониторинга судов «Виктория». URL = http://victoria.marsat.ru/ (дата обращения: 01.08.2018).
9. КИИС «МоРе». URL = http://www.marsat.ru/ciis-more (дата обращения: 01.08.2018).
10. ЕСИМО. URL = http://portal.esimo.ru/portal (дата обращения: 01.08.2018).
11. Система КОСПАС-САРСАТ. URL = https://www.cospas-sarsat.int/ru/ (дата обращения: 01.08.2018).
12. Программный комплекс «Поиск-Море». URL = http://map.geopallada.ru/ (дата обращения: 01.08.2018).
13. Introducing JSON. 2014. URL = http://www.json.org/ (дата обращения: 01.08.2018).
14. *Dmitriy Deviatkin, Artem Shelmanov* Towards Text Processing System for Emergency Event Detection in the Arctic Zone // Труды XVIII Междунар. конф. «Аналитика и управление данными в областях с интенсивным использованием данных DAMDID/RCDL′2016» (Ершово, 11−14 октября 2016 г., Россия) / Под ред. *Л.А. Калиниченко*, *Я. Манолопулоса*, *С.О. Кузнецова*. М.: ФИЦ ИУ РАН. 2016. С. 225−232.
15. *Девяткин Д.А.*, *Шелманов А.О.* Применение методов интеллектуального анализа текстов в задаче мониторинга чрезвычайных ситуаций в Арктической зоне // Системы высокой доступности. 2017. Т. 13. № 2. С. 45−55.
16. Annotation Query Language (AQL) reference. URL = https://www.ibm.com/support/knowledgecenter/SSPT3X_4.1.0/com.ibm.swg.im.infosphere.biginsights.aqlref.doc/doc/aql-overview.html (дата обращения: 01.08.2018).

17. *Beyer K.S.*, *Ercegovac V.*, *Gemulla R.*, *Balmin A.*, *Eltabakh M.*, *Kanne C.-C.*, *Ozcan F.*, *Shekita E.J.* Jaql: A Scripting Language for Large Scale Semistructured Data Analysis. VLDB 2011.
18. *Hernández M.*, *Koutrika G.*, *Krishnamurthy R.*, *Popa L.*, *Wisnesky R.* HIL: a high-level scripting language for entity integration // Proc. of the 16th International Conference on Extending Database Technology EDBT 2013. P. 549–560.
19. *Abrial J.-R.* The B-Book: Assigning Programs to Meanings. Cambridge: Cambridge University Press. 1996.
20. Atelier B, the industrial tool to efficiently deploy the B Method. URL = http://www.atelierb.eu/ (дата обращения: 01.08.2018).

Поступила 18 сентября 2018 г.

Implementation of methods for data integration and warehousing aimed at support of search and rescue operations in Arctic region

D.O. Briukhov – Ph.D.(Eng.), Senior Research Scientist, Institute of Informatics Problems of FRC CSC RAS (Moscow)
E-mail: dbriukhov@ipiran.ru
N.A. Skvortsov – Research Scientist, Institute of Informatics Problems of FRC CSC RAS (Moscow)
E-mail: nskv@ipi.ac.ru
S.A. Stupnikov – Ph.D.(Eng.), Senior Research Scientist, Institute of Informatics Problems of FRC CSC RAS (Moscow)
E-mail: sstupni-kov@ipiran.ru

Diversity of data sources on Arctic region that can be used for planning of search and rescue operations is quite significant. That is why the problem of development of data integration methods for this area is urgent. This paper presents an approach for implementation of methods for data integration into a unified warehouse. In particular, the following issues are considered: extraction of structured data from text documents, transformation of data into warehouse schema, fusion of data from various sources to create integrated entities, data integration program verification, warehouse implementation, loading of integrated data into the warehouse. Examples of analytical queries over warehouse schema that can be used for planning of search and rescue operations are presented.

References

1. *Bryuxov D.O.* Istochniki danny'x dlya informaczionnoj podderzhki poiskovo-spasatel'ny'x operaczij // Sistemy' vy'sokoj dostupnosti. 2015. T. 11. № 4. S. 83–89.
2. *Bryuxov D.O.*, *Skvorczov N.A.*, *Stupnikov S.A.* Metody' integraczii raznostrukturirovanny'x danny'x po Arkticheskoj zone dlya izvlecheniya informaczii, naczelennoj na podderzhku poiskovo-spasatel'ny'x operaczij // Sistemy' vy'sokoj dostupnosti. 2017. T. 13. № 2. S. 3–19.
3. *White T.* Hadoop: The Definitive Guide. Third Edition. O'Reilly Media. 2012.
4. *Skvorczov N.A.*, *Bryuxov D.O.* Razrabotka sxemy' xranilishha danny'x dlya podderzhki poiskovy'x dejstvij v Arkticheskoj zone // Sistemy' vy'sokoj dostupnosti. 2017. T. 13. № 2. S. 20–44.
5. *Capriolo E.*, *Wampler D.*, *Rutherglen J.* Programming Hive Data Warehouse and Query Language for Hadoop. O'Reilly Media. 2012.
6. *Miner D.* MapReduce Design Patterns: Building Effective Algorithms and Analytics for Hadoop and Other Systems. O'Reilly Media. 2012.
7. *Stupnikov S.* Semantics and Verification of Entity Resolution and Data Fusion Operations via Transformation into a Formal Notation // In: Data Analytics and Management in Data Intensive Domains. DAMDID/RCDL 2016. Communications in Computer and Information Science / Ed. by *L. Kalinichenko*, *S. Kuznetsov*, *Y. Manolopoulos*. Springer. 2017. V. 706. P. 145–162.
8. Sistema monitoringa sudov «Viktoriya». URL = http://victoria.marsat.ru/ (data obrashheniya: 01.08.2018).
9. KIIS «MoRe». URL = http://www.marsat.ru/ciis-more (data obrashheniya: 01.08.2018).
10. ESIMO. URL = http://portal.esimo.ru/portal (data obrashheniya: 01.08.2018).
11. Sistema KOSPAS-SARSAT. URL = https://www.cospas-sarsat.int/ru/ (data obrashheniya: 01.08.2018).
12. Programmny'j kompleks «Poisk-More». URL = http://map.geopallada.ru/ (data obrashheniya: 01.08.2018).
13. Introducing JSON. 2014. URL = http://www.json.org/ (data obrashheniya: 01.08.2018).
14. *Dmitriy Deviatkin, Artem Shelmanov* Towards Text Processing System for Emergency Event Detection in the Arctic Zone // Trudy' XVIII Mezhdunar. konf. «Analitika i upravlenie danny'mi v oblastyax s intensivny'm ispol'zovaniem danny'x DAMDID/RCDL'2016» (Ershovo, 11–14 oktyabrya 2016 g., Rossiya) / Pod red. *L.A. Kalinichenko*, *Ya. Manolopulosa*, *S.O. Kuzneczova*. M.: FICz IU RAN. 2016. S. 225–232.
15. *Devyatkin D.A.*, *Shelmanov A.O.* Primenenie metodov intellektual'nogo analiza tekstov v zadache monitoringa chrezvy'chajny'x situaczij v Arkticheskoj zone // Sistemy' vy'sokoj dostupnosti. 2017. T. 13. № 2. S. 45–55.
16. Annotation Query Language (AQL) reference. URL = https://www.ibm.com/support/knowledgecenter/SSPT3X_4.1.0/com.ibm.swg.im.infosphere.biginsights.aqlref.doc/doc/aql-overview.html (data obrashheniya: 01.08.2018).
17. *Beyer K.S.*, *Ercegovac V.*, *Gemulla R.*, *Balmin A.*, *Eltabakh M.*, *Kanne C.-C.*, *Ozcan F.*, *Shekita E.J.* Jaql: A Scripting Language for Large Scale Semistructured Data Analysis. VLDB 2011.
18. *Hernández M.*, *Koutrika G.*, *Krishnamurthy R.*, *Popa L.*, *Wisnesky R.* HIL: a high-level scripting language for entity integration // Proc. of the 16th International Conference on Extending Database Technology EDBT 2013. P. 549–560.
19. *Abrial J.-R.* The B-Book: Assigning Programs to Meanings. Cambridge: Cambridge University Press. 1996.
20. Atelier B, the industrial tool to efficiently deploy the B Method. URL = http://www.atelierb.eu/ (data obrashheniya: 01.08.2018).

УДК 681.3

Элементы конфиденциальности и перспективы их применения в системах интенсивного использования данных

В.И. Будзко – д.т.н., академик Академии криптографии РФ, зам. директора по научной работе, Институт проблем информатики ФИЦ ИУ РАН (Москва);
профессор, Национальный исследовательский ядерный университет «МИФИ» (Москва)
E-mail: vbudzko@ipiran.ru
В.И. Королев – д.т.н., вед. науч. сотрудник, Институт проблем информатики ФИЦ ИУ РАН (Москва);
профессор, Финансовый университет при Правительстве Российской Федерации
E-mail: Vkorolev@ipiran.ru
В.Г. Беленков – к.т.н., вед. науч. сотрудник, Институт проблем информатики ФИЦ ИУ РАН (Москва)
E-mail: vbelenkov@ipiran.ru

Рассмотрены перспективы применения встроенных элементов конфиденциальности для обеспечения информационной безопасности систем, реализующих интенсивное использование данных.

Ключевые слова: *элемент конфиденциальности, информационная безопасность, интенсивное использование данных.*

The article is devoted to the prospects of using built-in elements of confidentiality to ensure information security systems that implement intensive use of data.

Keywords: *privacy element, information security, data intensive domains.*

DOI: 10.18127/j20729472-201804-10

Системы интенсивного использования данных – автоматизированные информационные системы, обеспечивающие анализ и управление данными, обработку информации и решение функциональных исследовательских и прикладных задач в различных областях с интенсивным использованием данных (*Data Intensive Domains – DID*). Как правило, такие области связаны со сложившейся глобальной тенденцией создания массивных коллекций данных и обеспечения возможности их совместного использования при решении задач исследования и принятия решений [2, 3].

Практически в информационных технологиях сложился отдельный вид систем, который в дальнейшем будем именовать *DID-системами* (*системы функционирования в областях с интенсивным использованием данных*). В DID-системах может обрабатываться как открытая информация, так и информация, включающая в себя подлежащие защите сведения, относящиеся в соответствии с законодательством РФ к государственной или иной тайне, а также персональные данные. В зависимости от области применения и содержания обрабатываемой информации DID-системы могут создаваться как в открытом, так и в защищенном исполнении. Сущность протекающих в DID-системах процессов позволяет на уровне инфраструктурного и технологического представления соотнести их с системами *Big Data* с учетом их функциональных целей и особенностей построения.

DID-системы, являясь разновидностью автоматизированных систем (АС), должны отвечать требованиям информационной безопасности (ИБ), соответствующим классу защиты АС в части обеспечения целостности, доступности и конфиденциальности информации. Для обеспечения ИБ (ОИБ) должны быть решены соответствующие системно-технологические проблемы:

обеспечение системности и комплексности безопасности;

защита технологических (прикладных) процессов;

соответствие уровня защиты информации ценности, которой обладает эта информация;

защита информации без существенного снижения функциональных, операционных и временных характеристик АС;

доступность работы пользователей с ресурсами АС в соответствии с их правами и полномочиями;

бесперебойное функционирование АС в условиях угроз, воздействий и др.

Однако DID-системы имеют и свои особенности ОИБ в процессах обработки информации и ее применения. Они связаны, во-первых, с характеристиками информационных ресурсов (ИР) и, во-вторых, со свойствами конфиденциальности информации в них.

В первом случае необходимо отметить, что ИР DID-систем существенно отличаются от используемых ИР в традиционных аналитических системах по следующим основным характеристикам:

1) в DID-системах имеет место высокая концентрация информации, объемы обрабатываемых данных существенно превосходят аналогичные объемы для традиционных аналитических систем, поэтому ущерб их потери, искажения или блокирования доступа в значимых целевых задачах анализа и исследования возрастает, вплоть до критичного уровня;

2) массово применяются технологии распределенных вычислений и, как следствие, образуется большое число межсистемных и внутрисистемных связей информационного взаимодействия через сеть, вследствие чего повышаются требования по обеспечению целостности информации.

Во втором случае особенность может быть сформулирована как *проблема неопределенности категории доступа к информации* [1], получаемой в ходе сбора, переработки и получения информационного продукта. Даже если производится обработка данных, получаемых исключительно из общедоступных источников, в процессе их переработки и систематизации могут сформироваться сведения, доступ к которым ограничен в соответствии с федеральными законами. В этом случае конечный информационный продукт должен рассматриваться его обладателем как конфиденциальный [4].

Перечисленные факторы, связанные с особенностями ОИБ в DID-системах, порождают ряд частных проблем:

необходимость выделения и контроля информационных объектов, требующих защиты;

предоставление пользователю в результате обработки только тех сведений, к которым он имеет допуск, из всего найденного пула запрашиваемых сведений;

появление при поступлении исходных данных из источников либо при обработке запросов сведений, требования по защите которых превосходят возможности класса защиты DID-системы;

поступление при информационно-телекоммуникационном взаимодействии в информационном потоке сведений, требования по защите которых превосходят возможности, предусмотренные протоколом взаимодействия.

Решение этих частных проблем и проблемы в целом обусловили необходимость введения понятия *элемента конфиденциальности* (*ЭК*).

В настоящее время ОИБ в целом в DID-системах осуществляется, в первую очередь, за счет архитектурных решений, применяемых при их построении, а также за счет использования традиционных технологий защиты информации. Основные усилия разработчиков решений по ОИБ направлены на обеспечение высокой доступности информации [5, 6]. Обеспечение целостности информации в системах этого вида нацелено, прежде всего, на сохранение ее достоверности и обоснованности [7, 8].

Цель работы – рассмотреть возможный подход к решению проблемы *неопределенности категории доступа к информации*, получаемой в ходе сбора, переработки и формирования информационного продукта в системах интенсивного использования данных.

Концептуальные вопросы введения элементов конфиденциальности

Базовой задачей ОИБ в АС является задача управления разграничением доступа к информации, регулирование доступа к которой определяется законодательно. Это информация, содержащая сведения, отнесенные к определенным видам тайн (государственная, коммерческая, банковская, персональные данные и др.).

Для управления разграничением доступа необходимо иметь правовое поле отношений доступа между информационными объектами и субъектами-пользователями. Основными источниками ИР DID-систем являются массивы коллекций неструктурированных данных, в которых проблема идентификации информационных объектов ограниченного доступа принципиально не решена. Поэтому сформировать правовое поле в режиме детерминированного моделирования или путем прогнозирования весьма затруднительно. Как следствие, при создании банка данных DID-систем или при использовании внешних ИР в процессе решения функциональных аналитических задач необходимо научить систему извлекать и идентифицировать информационные объекты ограниченного доступа. В этих целях сформу-

лируем систему взаимосвязанных понятий, по своей природе аналогичных решению задачи извлечения знаний из контента.

Под *артефактом* будем понимать обособленный каким-либо образом контент или фрагмент контента, рассматриваемый как единое целое совместно с комплексом сопровождающих его учетных данных и контейнером, в котором размещен контент и комплекс сопровождающих его учетных данных.

Под *элементом конфиденциальности* (*ЭК*) понимается минимальная выборка (например, слово или другие атрибуты) из области контента, позволяющая с учетом ее положения в контенте отнести содержащиеся в артефакте сведения к защищаемым сведениям в конкретных областях деятельности. ЭК должен обеспечивать однозначное соответствие между артефактом и его уровнем конфиденциальности.

Входной контент DID-систем поступает из различных источников исходных данных (ИИД). Он может иметь различные формы представления: базы данных, файловые системы, веб-сайты и их страницы, геоинформационные системы, спутниковые и потоковые информационные системы, системы документооборота, а также данные электронных почт, социальных сетей, фото- и видеохостингов, блогов, машиноформируемых файлов и др.

Виды представления выходного контента DID-систем – это тексты, таблицы, электронные таблицы, диаграммы, графики, рисунки, ситуационная обстановка на карте, подсветка регионов на карте и другие формы отображения информации.

В качестве контейнеров рассматриваются сообщение, файл, в том числе архивный файл, папка, база данных, ее структурный элемент, сайт, портал, веб-страница и т.п. В общем случае контейнеры могут быть вложенными.

Наполнение ЭК может быть представлено в артефактах в явном виде, либо может быть получено из них методами извлечения знаний. При этом может использоваться смысловая обработка на основе таких моделей, как семантические и концептуальные сети, фреймы и т.д.

В зависимости от места нахождения ЭК подразделяются на *основные* и *дополнительные*.

Основные ЭК относятся непосредственно к контенту или к комплексу сопровождающих его данных. Они извлекаются из выделенных фрагментов, либо в целом из контента или сопровождающих его данных, а также из наименований контента или комплекса сопровождающих его данных.

Дополнительные ЭК относятся непосредственно к транспортировке и описанию артефактов, содержащих контент, а также к наименованиям ИИД и описаниям областей деятельности, к которым относятся эти источники или по которым поступают сведения из этих источников. Они извлекаются из транспортных контейнеров контента или комплекса сопровождающих его данных, а также из транспортных сообщений, сопровождающих эти контейнеры в соответствии с протоколом взаимодействия. Могут формироваться как на стороне DID-системы, так и на стороне ИИД.

Как основные, так и дополнительные ЭК могут быть заданы в явном виде как некоторые сигнатуры артефакта или определяться на основании анализа сведений, содержащихся в артефакте или в его окружении. ЭК идентифицируют необходимость защиты содержащихся в артефакте сведений и уровень допуска к ним (уровень конфиденциальности), а также могут характеризовать область деятельности или объект, к которому относятся защищаемые сведения.

Элемент конфиденциальности – это результат извлечения из артефакта знания о наличии в нем сведений, требующих защиты, и об отнесении их к определенному уровню конфиденциальности. Для его натурализации как реальной характеристики доступа к информации необходима идентификация результата, соотнесение его с некоторым эталоном. С этой целью введем понятие эталонного показателя ЭК (*эталонный ЭК*). Он является характеристической частью отнесения сведений из артефакта к защищаемым сведениям по определенному уровню конфиденциальности. Фактически это *сигнатуры доступа*.

Для понимания сущности эталонных ЭК обратимся к технологиям определения грифа секретности (конфиденциальности) в традиционных документах «ручного» документооборота. При определении грифа секретности (уровня конфиденциальности) документа используются официальные нормативные документы, включающие в себя *Перечни сведений, относящихся к государственной (коммерческой, банковской, медицинской и пр.) тайне*. Порядок включения сведений в эти Перечни носит характер достаточно субъективного и эвристического процесса, хотя критерии включения конкретны и связаны либо с областью деятельности и ее результатами, либо с объектами и процессами деятельности, либо с некоторыми обстоятельствами реалий. Тем не менее, перечень носит административно-правовой статус

обязательного применения.

Из этой аналогии следует необходимость создания *базы данных эталонных ЭК* для DID-системы в области решаемых информационно-аналитических задач.

Элементы конфиденциальности рассматриваются совместно с правилами их обработки. Правила обработки касаются таких аспектов, как:

определение области(ей) поиска ЭК в артефактах;

отнесение содержащейся в артефакте информации к защищаемым сведениям;

форма учета необходимости защиты сведений при размещении артефактов в интегрированном хранилище данных (ИХД), либо при представлении пользователю результатов обработки его запроса;

алгоритмы и технологии обработки.

Правила обработки ЭК определяются протоколами информационно-технологического взаимодействия и протоколами (требованиями) по ОИБ регуляторов ИБ. Правила группируются в совокупности: связанные с ИИД, областями деятельности, видами объектов, видами объектов в областях деятельности, видами артефактов и т.п.

Области применения элементов конфиденциальности в информационных технологиях

В системе обеспечения информационной безопасности (СОИБ) DID-систем ЭК целесообразно использовать при решении задач предотвращения несанкционированного доступа к сведениям, охраняемым в различных областях деятельности, а также предотвращения поступления в DID-систему сведений, уровень секретности/конфиденциальности которых превосходит возможности системы по защите информации.

Можно выделить *три основных области информационных технологий*, в которых использование ЭК целесообразно и необходимо.

1. *При взаимодействии DID-системы с ИИД и при размещении данных в системе* ЭК целесообразно использовать для контроля соблюдения протокола информационно-телекоммуникационного взаимодействия ИИД с DID-системой, а также для определения необходимости защиты сведений, содержащихся в конкретных артефактах, и уровня допуска к ним. При этом в DID-системе сведения хранятся в соответствии с ЭК, определяющими уровень допуска к этим сведениям, или вместе с этими ЭК.

2. *При выдаче пользователям результатов выполнения их запросов* ЭК целесообразно использовать для определения необходимости защиты предоставляемых сведений, содержащихся в результатах выполнения конкретного запроса, и уровня допуска к ним, а также соответствия этому уровню прав пользователя, выдавшего запрос.

3. *При обработке запросов пользователей* ЭК целесообразно использовать для определения областей ИХД и структурированных хранилищ данных, доступных для конкретного пользователя в соответствии с его правами доступа к данным.

Общая технологическая схема применения элементов конфиденциальности

Использование ЭК осуществляется с учетом контекста, соответствующего областям деятельности. В такой контекст входят обладатели и пользователи данных, объекты или системы, к которым относятся данные, и связанные с ними ограничения по обеспечению конфиденциальности.

Сущность контекста определяется:

1) протоколами информационно-телекоммуникационного взаимодействия DID-системы с ИИД;

2) протоколами по ОИБ DID-системы с регулятором ИБ в области деятельности.

Обработка ЭК должна осуществляться на выделенных аппаратно-программных комплексах (АПК-ЭК). Необходимость создания выделенных АПК обусловлена тем, что определение для конкретного артефакта уровня допуска, включая деятельность экспертов и контролеров ИБ DID-системы, в общем случае связана с обработкой сведений, уровень допуска к которым выше уровня допуска DID-системы. АПК должен осуществлять предобработку артефактов, поступающих из ИИД в DID-систему, а также постобработку результатов выполнения запросов перед передачей этих результатов пользователю.

При этом каждый артефакт, принятый DID-системой перед его содержательной обработкой, после

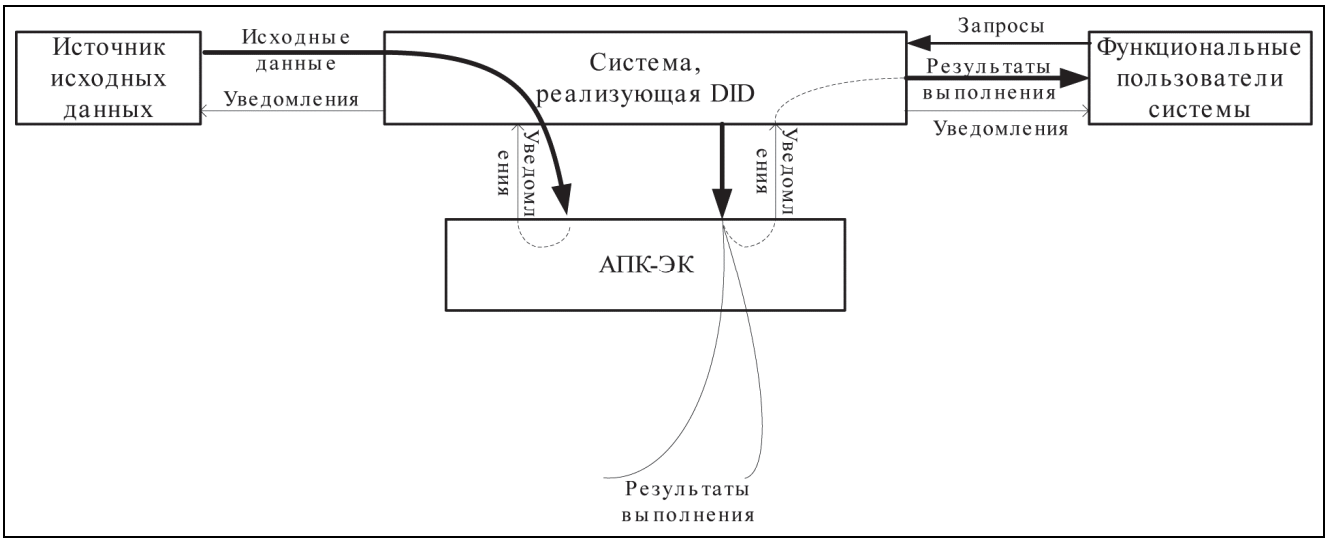

Схема ОИБ в технологическом процессе обработки больших объемов данных DID-системой

АПК-ЭК передается в систему для определения его уровня допуска или его общедоступности. По результатам его обработки АПК-ЭК передает в DID-систему уведомление, содержащее обезличенный технологический идентификатор артефакта, а также уровень допуска артефакта и область деятельности, к которой он относится, либо код инцидента, связанного с нарушением показателя уровня допуска ЭК (назовем этот инцидент ИБэк). Также АПК может передавать детализирующие сведения.

Аналогично, результаты выполнения DID-системой каждого запроса пользователя перед их предоставлением пользователю передаются системой в АПК-ЭК для определения их уровня допуска или их общедоступности. По результатам формируется уведомление об уровне допуска к результату, либо код инцидента ИБэк.

Место АПК-ЭК в технологическом процессе обработки данных DID-системой иллюстрируется схемой, приведенной на рисунке.

- Развитие информационных технологий, становление информационного общества порождают принципиально новые и все более сложные вызовы, связанные с ОИБ. Одним из важных исходных факторов данного процесса является глобальная тенденция создания массивных коллекций неструктурированных данных и их широкое совместное использование в задачах исследования и принятия решений. При этом так сложилось в мировой практике информатизации и автоматизации, что вопросы реализации новых информационных технологий и вопросы ОИБ далеки от приемлемого состояния взаимосвязанного развития.

  Был рассмотрен один из аспектов решения базовой задачи ОИБ – управления разграничением доступа в информационно-аналитических системах с интенсивным использованием больших данных. На концептуальном уровне выполнена постановка задачи использования для разграничения доступа ЭК, описаны перспективы их использования для ОИБ данного вида систем.

  Актуальность использования ЭК связана с наличием проблемы неопределенности категории доступа к информации в этих системах, при которой невозможно создать правовое поле доступа к ИР.

  В статье введено понятие ЭК для информационных объектов, выполнена постановка задачи их использования при извлечении информации и последующей интеграции данных, предложен общий подход к технологии их внедрения в информационные процессы с целью ОИБ, приведены виды ЭК.

Литература

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации».
2. *Калиниченко Л.А.*, *Вольнова А.А.*, *Гордов Е.П. и др.* Проблемы доступа к данным в исследованиях с интенсивным использованием данных в России // Информатика и ее применения. 2016. Т. 10. № 1. С. 3–23.

3. *Будзко В.И.*, *Беленков В.Г.*, *Борохов С.В.* Проблемы обеспечения информационной безопасности при интенсивном использовании данных // Труды Междунар. научно-технич. конф. «Информационные технологии и математическое моделирование систем 2017». М.: Центр информационных технологий в проектировании РАН. 2017. С. 122–124.
4. *Беленков В.Г.*, *Борохов С.В.*, *Будзко В.И.*, *Кейер П.А.*, *Королев В.И.* Вопросы обеспечения информационной безопасности информационных систем, реализующих интенсивное использование данных // Сб. науч. трудов XIX Междунар. конф. «Аналитика и управление данными в областях с интенсивным использованием данных DAMDID». RCDL'2017. 10–13 октября 2017 г., Москва, МГУ, Россия / Под ред. *Л.А. Калиниченко*, *Я. Манолопулос*, *Н.А. Скворцова*, *В.А. Сухомлина*. М.: ФИЦ ИУ РАН. 2017. С. 155–158.
5. *Будзко В.И.*, *Кейер П.А.* Новые подходы к обеспечению информационной безопасности в телекоммуникационных сетях // Труды Междунар. научно-технич. конф. «Информационные технологии и математическое моделирование систем 2017». М.: Центр информационных технологий в проектировании РАН. 2017. С. 83–85.
6. *Зацаринный А.А.*, *Королев В.И.* Особенности подготовки информационно-аналитического продукта средствами сегментированного ситуационного центра // Системы и средства информатики. 2017. Т. 27. № 4. С. 122–129.
7. *Zikopoulos P.C.*, *Eaton C.*, *deRoos D.*, *Deutsch T.*, *Lapis G.* Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data. The McGraw-Hill Companies. 2012. 141 p.
8. *Zikopoulos P.C.*, *deRoos D.*, *Parasuraman K.*, *Deutsch T.*, *Corrigan D.*, *Giles J.* Harness the Power of Big Data The IBM Big Data Platform. The McGraw-Hill Companies. 2013. 242 p.

Поступила 18 сентября 2018 г.

Privacy elements and prospects of their use in data intensive systems

V.I. Budzko – Dr.Sc.(Eng.), Member of Russian Cryptography Academy, Deputy Director on Research and Development, Institute of Informatics Problems of FRC CSC RAS (Moscow);
Professor, National Research Nuclear University «MEPhI» (Moscow)
E-mail: vbudzko@ipiran.ru
V.I. Korolev – Dr.Sc.(Eng.), Leading Research Scientist, Institute of Informatics Problems of FRC CSC RAS (Moscow);
Professor, Financial University under the Government of the Russian Federation
E-mail: Vkorolev@ipiran.ru
V.G. Belenkov – Ph.D.(Eng.), Leading Research Scientist, Institute of Informatics Problems of FRC CSC RAS (Moscow)
E-mail: vbelenkov@ipiran.ru

The article deals with the features and problems of information security in the areas of data intensive use (Data Intensive Domains – DID). Approaches to information security for systems operating in the areas of intensive data use are noted. Conceptual issues of introduction of confidentiality elements into information technology processes are considered. The task of using elements of confidentiality in the elemention of information and subsequent data integration is formulated. The use of privacy elements to solve information security problems in the accumulation of information and its elemention is described. The types of elements of confidentiality, their main indicators and characteristics are given.

References

1. Federal law № 149-FZ of 27 July 2006 «On information, information technologies and protection of information».
2. *Kalinichenko L.A., A.A. Volnova, Gordov E.P. etc.* The problems of data access in research with Data Intensive Domain // Informatics and its applications. 2016. V. 10. № 1. P. 3–23.
3. *Budzko V.I., Belenkov V.G., Borokhov S.V.* The problems of information security in Data Intensive Domain // Proc. of the International scientific and technical conference «Information technologies and mathematical modeling of systems 2017». M.: Center of information technologies in the design of RAS. 2017. P. 122–124.
4. *Belenkov V.G., Borokhov S.V., Budzko V.I., Keyer P.A., Korolev V.I.* Issues of information security of information systems implementing Data Intensive Domain. // Collection of scientific papers of the XIX International conference «Analytics and data management in areas with Data Intensive Domain DAMDID». RCDL'2017. 10–13 October 2017, Moscow, MSU, Russia / Ed. by *L.A. Kalinichenko*, *I. Manolopoulos*, *N. Skvortsova*, *V.A. Sukhomlin*. M. FIC IU RAS. 2017. P. 155–158.
5. *Budzko V.I., Keyer P.A.* New approaches to information security in telecommunication networks // Proc. of the International scientific and technical conference «Information technologies and mathematical modeling of systems 2017». M.: Center of information technologies in the design of RAS. 2017. P. 83–85.
6. *Zatsarinny A.A. and Korolev V.I.* The features of information and analytical product preparation by means of the segmented situation center // Systems and Means of Informatics. 2017. V. 27. № 4. P. 122–131.
7. *Zikopoulos P.C., Eaton C., deRoos D., Deutsch T., Lapis G.* Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data. The McGraw-Hill Companies. 2012. 141 p.
8. *Zikopoulos P.C., deRoos D., Parasuraman K., Deutsch T., Corrigan D., Giles J.* Harness the Power of Big Data. The IBM Big Data Platform. The McGraw-Hill Companies. 2013. 242 p.

УДК 004.056.55

Квантовая криптографическая система АКМ2017 на основе ресурса несепарабельности состояния спиновой синглет

Ф.К. Алиев – д.ф.-м.н., вед. советник, Главное управление развития информационных и телекоммуникационных технологий МО РФ
А.В. Корольков – к.т.н., доцент, зав. кафедрой, чл.-корр. Академии криптографии РФ, РТУ МИРЭА (Москва); зав. лабораторией, Академия криптографии РФ
Е.А. Матвеев – директор НТП «Криптософт» (г. Пенза)
С.С. Орлов – сотрудник, Изд-во ТВП (Москва)
И.А. Шеремет – чл.-корр. РАН, д.т.н., профессор, зам. директора РФФИ (Москва)

Представлены основные положения новой квантовой криптографической системы АКМ2017, основанной на использовании квантового ресурса несепарабельности состояния спиновой синглет. Приведены результаты сравнительного анализа АКМ2017 по отношению как к классическим криптографическим системам, так и к известным квантовым криптографическим системам. Показано, что криптографическая система АКМ2017 может служить еще одним подтверждением тезиса о том, что квантовые компьютерные технологии дают больше преимуществ защите информации, чем действиям по ее преодолению.

Ключевые слова: *квантовая криптография, криптографическая система, квантовый компьютер, кубит, квантовая система, несепарабельные (запутанные) состояния, теоретическая стойкость, криптографическая техника, состояние спиновой синглет, измерение компоненты спина вдоль оси.*

The article presents the main provisions of the new quantum cryptographic system AKM2017, based on the use of the quantum resource of non-separability of the spin singlet state. The results of the comparative analysis of AKM2017 in relation to both classical cryptographic systems and known quantum cryptographic systems are presented. It is pointed out that the cryptographic system AKM2017 can serve as another confirmation of the thesis that quantum computer technologies give more advantages to information protection than actions to overcome it.

Keywords: *quantum cryptography, cryptographic system, quantum computer, qubit, quantum system, inseparable (entangled) states, theoretical stability, cryptographic technique, spin singlet state, measurement of spin components along the axis.*

DOI: 10.18127/j20729472-201804-11

Возможное появление широко рекламируемых в последние годы квантовых технологий обработки информации и квантовых вычислительных устройств может внести существенные коррективы в существующее положение в области информационной безопасности как в России, так и во всем мире. Прогнозируют многократное увеличение числа как мнимых, так и действительных угроз. Считается, что появление «полноценного квантового компьютера» сведет на нет возможности обеспечения информационной безопасности путем применения асимметричных криптографических систем и симметричных криптографических систем с ограниченной длиной ключа, не являющихся теоретически стойкими. Такое развитие событий может привести к существенному уменьшению парка криптографической техники, пригодной для практических применений. При этом бескомпромиссную надежность сохраняет лишь имеющая соответствующее заключение регулятора криптографическая техника, в которой реализованы теоретически стойкие криптографические алгоритмы.

Теоретически стойкие криптографические системы (по Шеннону, совершенные шифры [17]) при всех своих отличных показателях по стойкости обладают рядом недостатков, существенно затрудняющих их практическое применение в области обеспечения информационной безопасности. Самым значимым среди них является сложность подсистемы управления ключами, под которой понимается подсистема генерации, распределения, применения и утилизации ключевой информации. Как правило, по причине сложности подсистемы управления ключами теоретически стойкие криптографические системы являются громоздкими в практической эксплуатации, дорогими по затратам при выработке и распределении ключевой информации и подвержены повышенной опасности компрометации ключевой информации вне контролируемых зон. Поэтому они имеют ограниченное применение.

Сказанное свидетельствует об актуальности разработки и применения новых механизмов защиты информации, устойчивых как к известным в настоящее время угрозам, так и к тем, которые обуславливаются предполагаемым появлением квантовых вычислительных устройств. Одним из перспективных путей в этом направлении может служить разработка и широкое применение новых механизмов защиты информации, основанных на квантовых ресурсах, включая и те, которые не имеют аналогов в классической физике. Среди определенной части специалистов в области информационной безопасности распространено даже такое мнение, что грядущие квантовые технологии дают больше преимуществ для защиты информации, чем для действий по ее преодолению. Вполне может оказаться так (это подтверждают и результаты, представленные в данной статье), что новые механизмы могут противостоять вычислительной мощи квантовых компьютеров с эффективностью не менее, чем теоретически стойкие классические криптографические системы, и, в то же самое время, лишены их недостатков, препятствующих полноценному широкому практическому использованию.

Ц е л ь р а б о т ы – рассмотреть принципиально новую квантовую криптографическую систему *АКМ2017*.

В статье описаны свойства такого ресурса квантовой физики, как ресурс несепарабельности состояния квантовой системы из двух кубитов, известного под названием спиновой синглет [15]. Представлена новая теоретически стойкая квантовая криптографическая система АКМ2017, основанная на использовании ресурса несепарабельности состояния спиновой синглет. Проведен сравнительный анализ АКМ2017 с известными криптографическими системами. Акцентируется внимание на новых качественных свойствах квантовой криптографической системы АКМ2017. Совокупность этих свойств невозможна в принципе как для классических криптографических систем, так и (в смысле всей своей исчерпывающей полноты) для известных ранее систем квантовой криптографии.

1. Состояние спиновой синглет. Теоретические основы

Рассмотрим состояние Белла двухкубитной квантовой системы AB

$$\left|\psi_{11}\right\rangle = \frac{\left|01\right\rangle - \left|10\right\rangle}{\sqrt{2}}. \tag{1}$$

По историческим причинам это состояние принято называть *спиновым синглетом* [15].

Обратим внимание на обозначение $\left|\kappa_1\kappa_2\cdots\kappa_r\right\rangle$:

$$\left|\kappa_1\kappa_2\cdots\kappa_r\right\rangle = \left|\kappa_1\right\rangle\left|\kappa_2\right\rangle \ \ldots\ \left|\kappa_r\right\rangle = \left|\kappa_1\right\rangle\otimes\left|\kappa_2\right\rangle\otimes\ \ldots\ \otimes\left|\kappa_r\right\rangle,$$

где $\kappa_1, \kappa_2, \ldots, \kappa_r \in \{0, 1\}$; $\left|0\right\rangle = \left|\uparrow\right\rangle = \begin{pmatrix}1\\0\end{pmatrix}$; $\left|1\right\rangle = \left|\downarrow\right\rangle = \begin{pmatrix}0\\1\end{pmatrix}$; r – произвольное натуральное число; $\otimes$ – знак тензорного произведения [16].

Как следует из [16], состояние $\left|\psi_{11}\right\rangle$ является несепарабельным состоянием квантовой системы из двух кубитов.

Напомним [1, 16], что под *измерением компоненты спина вдоль оси* **v**, где $\mathbf{v} = (v_1, v_2, v_3)$ – единичный вектор (то есть вектор **v** является нормированным вектором [16]) в трехмерном пространстве над полем действительных чисел $\mathbb{R}$, понимается измерение наблюдаемой:

$$\mathbf{v}\sigma = v_1\sigma_1 + v_2\sigma_2 + v_3\sigma_3, \tag{2}$$

где σ_1, σ_2, σ_3 – вентили Паули.

При этом вентиль σ_1 равен

$$\sigma_1 = \sigma_{\mathbf{X}} = \mathbf{X} = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}. \tag{3}$$

Он представляет собой квантовый аналог классического логического элемента NOT и действует на однокубитное состояние $\left|\psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$ (где $\alpha, \beta \in \mathbb{C}$, $\mathbb{C}$ – поле комплексных чисел, $\left|\alpha\right|^2 + \left|\beta\right|^2 = 1$) следующим образом:

$$\sigma_1|\psi\rangle = \sigma_{\mathbf{X}}|\psi\rangle = \mathbf{X}|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}|\psi\rangle = \beta|0\rangle + \alpha|1\rangle. \quad (4)$$

Вентиль σ_2 определяется так:

$$\sigma_2 = \sigma_{\mathbf{Y}} = \mathbf{Y} = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}. \quad (5)$$

Он действует на однокубитное состояние $|\psi\rangle$ таким образом:

$$\sigma_2|\psi\rangle = \sigma_{\mathbf{Y}}|\psi\rangle = \mathbf{Y}|\psi\rangle = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}|\psi\rangle = -\beta\mathrm{i}|0\rangle + \alpha\mathrm{i}|1\rangle, \quad (6)$$

где $\mathrm{i} \in \mathbb{C}$, i – мнимая единица, то есть $\mathrm{i}^2 = -1$.

Вентиль σ_3 определяется выражением

$$\sigma_3 = \sigma_{\mathbf{Z}} = \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (7)$$

Он действует на однокубитное состояние $|\psi\rangle$ так:

$$\sigma_3|\psi\rangle = \sigma_{\mathbf{Z}}|\psi\rangle = \mathbf{Z}|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}|\psi\rangle = \alpha|0\rangle - \beta|1\rangle. \quad (8)$$

Для наблюдаемой $\mathbf{v}\sigma$ имеют место равенства

$$\mathbf{v}\sigma = v_1\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + v_2\begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} + v_3\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} v_3 & v_1 - \mathrm{i}v_2 \\ v_1 + \mathrm{i}v_2 & -v_3 \end{pmatrix}. \quad (9)$$

Вычислим характеристический многочлен $\chi_{\mathbf{v}\sigma}(\lambda)$ полученной матрицы (9) (учитывая, что $v_1^2 + v_2^2 + v_3^2 = 1$): $\chi_{\mathbf{v}\sigma}(\lambda) = \begin{vmatrix} \lambda - v_3 & -v_1 + \mathrm{i}v_2 \\ -v_1 - \mathrm{i}v_2 & \lambda + v_3 \end{vmatrix} = \lambda^2 - 1.$

Отсюда следует, что возможные значения наблюдаемой $\mathbf{v}\sigma$ независимо от значений координат единичного вектора $\mathbf{v} = (v_1, v_2, v_3)$ равны

$$\lambda_{1,2} = \pm 1. \quad (10)$$

Таким образом, при выполнении измерения компоненты спина вдоль оси $\mathbf{v}$ для обоих кубитов A и B (то есть измерения наблюдаемой $\mathbf{v}\sigma$ для каждого из кубитов A и B) получим для каждого из них «1» или «−1». Других значений быть не может, так как выше было показано, что возможные значения наблюдаемой $\mathbf{v}\sigma$ равны ±1 независимо от значений координат единичного вектора $\mathbf{v}$.

Имеет место очень важное утверждение, которое играет существенную роль в данной работе для построения квантовой криптографической системы АКМ2017 и обоснования ее свойств.

Перед формулировкой и доказательством этого утверждения проведем необходимые для дальнейшего вычисления, связанные с собственными состояниями $|a\rangle$ и $|b\rangle$, отвечающими соответственно собственным значениям «1» и «−1» наблюдаемой $\mathbf{v}\sigma$, а именно: выразим через координаты вектора $\mathbf{v}$ координаты состояний $|a\rangle$ и $|b\rangle$. И, кроме того, выразим векторы $|0\rangle$ и $|1\rangle$ через векторы $|a\rangle$ и $|b\rangle$.

Отдельно будем рассматривать т р и с л у ч а я в зависимости от значения координаты v_3 вектора $\mathbf{v}$: $v_3 = 1$, $v_3 = -1$, $v_3 \notin \{\pm 1\}$.

С л у ч а й 1. Пусть $v_3 = 1$. Тогда из равенства $v_1^2 + v_2^2 + v_3^2 = 1$ следует, что $v_1 = v_2 = 0$. Отсюда и из равенств (9) следует, что $\mathbf{v}\sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, что, в свою очередь, влечет справедливость равенств

$$|a\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |b\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \quad (11)$$

Из (11) следует, что

$$|0\rangle = |a\rangle, \quad |1\rangle = |b\rangle. \tag{12}$$

С л у ч а й 2 . Пусть $v_3 = -1$. Тогда из равенства $v_1^2 + v_2^2 + v_3^2 = 1$ следует, что $v_1 = v_2 = 0$. Отсюда и из равенств (9) следует, что $\mathbf{v}\sigma = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, что, в свою очередь, влечет справедливость равенств

$$|a\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad |b\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{13}$$

Из (13) следует, что

$$|0\rangle = |b\rangle, \quad |1\rangle = |a\rangle. \tag{14}$$

С л у ч а й 3 . Пусть $v_3 \notin \{\pm 1\}$.Тогда с учетом (9) из равенств

$$\mathbf{v}\sigma|a\rangle = |a\rangle, \quad \mathbf{v}\sigma|b\rangle = -|b\rangle \tag{15}$$

получаем

$$|a\rangle = \begin{pmatrix} \dfrac{v_1 - \mathrm{i}v_2}{\sqrt{(1-v_3)^2 + v_1^2 + v_2^2}} \\ \dfrac{1 - v_3}{\sqrt{(1-v_3)^2 + v_1^2 + v_2^2}} \end{pmatrix}, \quad |b\rangle = \begin{pmatrix} \dfrac{-v_1 + \mathrm{i}v_2}{\sqrt{(1+v_3)^2 + v_1^2 + v_2^2}} \\ \dfrac{1 + v_3}{\sqrt{(1+v_3)^2 + v_1^2 + v_2^2}} \end{pmatrix}. \tag{16), (17}$$

Из (16) и (17) следует, что

$$|0\rangle = \frac{(v_1 + \mathrm{i}v_2)(1+v_3)k_a}{2\left(v_1^2 + v_2^2\right)}|a\rangle + \frac{(v_1 + \mathrm{i}v_2)(-1+v_3)k_b}{2\left(v_1^2 + v_2^2\right)}|b\rangle, \quad |1\rangle = \frac{k_a}{2}|a\rangle + \frac{k_b}{2}|b\rangle, \tag{18}$$

где

$$k_a = \sqrt{(1-v_3)^2 + \left(v_1^2 + v_2^2\right)} = \sqrt{2 - 2v_3}, \quad k_b = \sqrt{(1+v_3)^2 + \left(v_1^2 + v_2^2\right)} = \sqrt{2 + 2v_3}, \tag{19}$$

Имеет место следующее утверждение.

Утверждение. Пусть квантовая система AB из двух кубитов A и B находится в состоянии $|\psi_{11}\rangle$, то есть в состоянии спиновой синглет. Тогда:

1) для любого единичного вектора $\mathbf{v} = (v_1, v_2, v_3)$ над полем действительных чисел $\mathbb{R}$ измерения наблюдаемой $\mathbf{v}\sigma$ для каждого из кубитов A и B (вне зависимости какой из них подвергается измерению первым, а какой – вторым) дают значение результата первого измерения, равное «1» или «−1» с вероятностью 0,5; а значение результата второго измерения с вероятностью 1 равно значению результата первого измерения с противоположным знаком;

2) для любого единичного вектора $\mathbf{v} = (v_1, v_2, v_3)$ над полем действительных чисел $\mathbb{R}$ измерения наблюдаемой $\mathbf{v}\sigma$ для кубита A и измерения наблюдаемой $(-\mathbf{v})\sigma$ для кубита B (вне зависимости какой из кубитов A и B подвергается измерению первым, а какой – вторым) дают значение результата первого измерения, равное «1» или «−1» с вероятностью 0,5; а значение результата второго измерения с вероятностью 1 равно значению результата первого измерения;

3) для любого единичного вектора $\mathbf{v} = (v_1, v_2, v_3)$ над полем действительных чисел $\mathbb{R}$ измерения сперва наблюдаемой $(0, 0, 1)\sigma$ для кубита A и затем измерение наблюдаемой $\mathbf{v}\sigma$ для того же кубита A дают значение результата первого измерения, равное «1» или «−1» с вероятностью 0,5; а при $v_3 \notin \{\pm 1\}$ результат второго измерения имеет следующее значение в зависимости от результата первого измерения:

если результат первого измерения равен «1», то результат второго измерения равен «1» с вероятно-

стью $P_A(1)$ или равен «−1» с вероятностью $P_A(-1)$, где

$$P_A(1) = \frac{k_b^2}{4} = \frac{1+v_3}{2}; \quad P_A(-1) = \frac{k_a^2}{4} = \frac{1-v_3}{2}; \tag{20}$$

если результат первого измерения равен «−1», то результат второго измерения равен «1» с вероятностью $P_A(1)$ или равен «−1» с вероятностью $P_A(-1)$, где

$$P_A(1) = \frac{k_a^2}{4} = \frac{1-v_3}{2}; \quad P_A(-1) = \frac{k_b^2}{4} = \frac{1+v_3}{2}; \tag{21}$$

4) для любого единичного вектора $\mathbf{v} = (v_1, v_2, v_3)$ (где $v_3 \notin \{\pm 1\}$) над полем действительных чисел $\mathbb{R}$ измерения сперва наблюдаемой $(0, 0, 1)\sigma$ для кубита A дает значение результата этого измерения, равное «1» или «−1» с вероятностью 0,5; и в этом случае последующее измерение наблюдаемой $\mathbf{v}\sigma$ для того же кубита A дает значение результата второго измерения, не зависящее от значения результата первого измерения и равное «1» или «−1» с вероятностью 0,5 тогда и только тогда, когда $v_3 = 0$.

Д о к а з а т е л ь с т в о .

1. Будем рассматривать отдельно случаи $v_3 = 1$, $v_3 = -1$ и $v_3 \notin \{\pm 1\}$.

Пусть $v_3 = 1$. В этом случае искомый результат очевидным образом следует из равенств (12).

Пусть $v_3 = -1$. В этом случае искомый результат очевидным образом следует из равенств (14).

Пусть $v_3 \notin \{\pm 1\}$. Тогда из равенств (18) следует, что

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} = k_{ab} \frac{|ab\rangle - |ba\rangle}{\sqrt{2}}, \tag{22}$$

где

$$k_{ab} = \frac{(v_1 + \mathrm{i}v_2)(1+v_3)k_a}{2\left(v_1^2 + v_2^2\right)} \frac{k_b}{2} - \frac{(v_1 + \mathrm{i}v_2)(-1+v_3)k_b}{2\left(v_1^2 + v_2^2\right)} \frac{k_a}{2} = (v_1 + \mathrm{i}v_2) \frac{k_a k_b}{2\left(v_1^2 + v_2^2\right)}. \tag{23}$$

Вычислим модуль $|k_{ab}|$ величины k_{ab}. Из определения модуля комплексного числа и равенств (19) следует, что

$$|k_{ab}| = \sqrt{v_1^2 + v_2^2} \frac{k_a k_b}{2\left(v_1^2 + v_2^2\right)} = \sqrt{v_1^2 + v_2^2} \frac{\sqrt{4\left(v_1^2 + v_2^2\right)}}{2\left(v_1^2 + v_2^2\right)} = 1. \tag{24}$$

Из равенств (22) и (24) следует, что состояния $\frac{|01\rangle - |10\rangle}{\sqrt{2}}$ и $\frac{|ab\rangle - |ba\rangle}{\sqrt{2}}$ совпадают с точностью до ненаблюдаемого при измерении общего множителя k_{ab}. Следовательно, если выполнено измерение наблюдаемой $\mathbf{v}\sigma$ для каждого из кубитов A и B (вне зависимости какой из кубитов A и B подвергается измерению первым, а какой – вторым), то результат «1» (или «−1»), полученный при первом измерении, приводит к результату «−1» (или «1») при втором измерении. Действительно, допустим для определенности, что первым измерению подвергался кубит A и получен результат «1». Тогда после этого измерения квантовая система AB из двух кубитов A и B окажется в состоянии $|ab\rangle$, что предопределяет значение «−1» результата второго измерения уже над кубитом B наблюдаемой $\mathbf{v}\sigma$, у которой состояние $|b\rangle$ отвечает собственному значению «−1».

Аналогично, если первым измерению подвергался кубит A и получен результат «−1», то после этого измерения квантовая система AB из двух кубитов A и B окажется в состоянии $|ba\rangle$, что предопределяет значение «1» результата второго измерения уже над кубитом B наблюдаемой $\mathbf{v}\sigma$, у которой состояние $|a\rangle$ отвечает собственному значению «1».

2. Из равенств (16) и (17) собственных состояний $|a\rangle$ и $|b\rangle$ наблюдаемой $\mathbf{v}\sigma$, отвечающих собственным значениям «1» и «−1» соответственно, следует, что те же векторы $|a\rangle$ и $|b\rangle$ являются собственными

состояниями наблюдаемой $(-\mathbf{v})\sigma$, отвечающими тем же собственным значениям, но в другом порядке следования, то есть «−1» и «1» соответственно. Тогда, если при измерении наблюдаемой $\mathbf{v}\sigma$ для кубита A получен результат, равный «1», то после измерения квантовая система AB из двух кубитов A и B окажется в состоянии $|ab\rangle$, что предопределяет значение «1» результата второго измерения наблюдаемой $(-\mathbf{v})\sigma$, у которой, как было показано, состояние $|b\rangle$ отвечает собственному значению «1».

Аналогично, если при измерении наблюдаемой $\mathbf{v}\sigma$ для кубита A получен результат, равный «−1», то после измерения квантовая система AB из двух кубитов A и B окажется в состоянии $|ba\rangle$, что предопределяет значение «−1» результата второго измерения наблюдаемой $(-\mathbf{v})\sigma$, у которой, как было показано, состояние $|a\rangle$ отвечает собственному значению «−1».

3. Из равенств (12) следует, что первое измерения наблюдаемой $(0, 0, 1)\sigma$ сначала для кубита A дает значение результата измерения, равное «1» или «−1» с вероятностью 0,5.

Если результат первого измерения над кубитом A равен «1», то после измерения квантовая система AB из двух кубитов A и B окажется в состоянии $|01\rangle = |0\rangle\otimes|1\rangle$, то есть кубит A окажется в состоянии $|0\rangle$, а кубит B – в состоянии $|1\rangle$. Для состояния $|0\rangle$ кубита A из условия $\mathbf{v}_3 \notin \{\pm 1\}$ и (18) следует справедливость равенства $|0\rangle = \frac{(v_1 + \mathrm{i}v_2)(1+v_3)k_a}{2\left(v_1^2+v_2^2\right)}|a\rangle + \frac{(v_1+\mathrm{i}v_2)(-1+v_3)k_b}{2\left(v_1^2+v_2^2\right)}|b\rangle$.

А так как измерение наблюдаемой $\mathbf{v}\sigma$ для кубита A в состоянии $|0\rangle$ означает проекционное измерение в базисе из векторов $|a\rangle$ и $|b\rangle$, то результат этого измерения равен «1» с вероятностью $P_A(1) = \frac{(1+v_3)^2 k_a^2}{4\left(v_1^2+v_2^2\right)}$ или «−1» с вероятностью $P_A(-1) = \frac{(-1+v_3)^2 k_b^2}{4\left(v_1^2+v_2^2\right)}$.

Подставив в правые части данных равенств вместо k_a и k_b их значения в соответствии с (19) и воспользовавшись затем равенством $v_1^2 + v_2^2 + v_3^2 = 1$, получаем:

$$P_A(1) = \frac{(1+v_3)^2\left[(1-v_3)^2 + \left(v_1^2+v_2^2\right)\right]}{4\left(v_1^2+v_2^2\right)} = \frac{1+v_3}{2}, \quad P_A(-1) = \frac{(-1+v_3)^2\left[(1+v_3)^2 + \left(v_1^2+v_2^2\right)\right]}{4\left(v_1^2+v_2^2\right)} = \frac{1-v_3}{2}.$$

Аналогично, если результат первого измерения равен «−1», то после измерения квантовая система AB из двух кубитов A и B окажется в состоянии $|10\rangle = |1\rangle\otimes|0\rangle$, то есть кубит A окажется в состоянии $|1\rangle$, а кубит B – в состоянии $|0\rangle$. Для состояния $|1\rangle$ кубита A из условия $v_3 \notin \{\pm 1\}$ и (18) следует справедливость равенства $|1\rangle = \frac{k_a}{2}|a\rangle + \frac{k_b}{2}|b\rangle$.

А так как измерение наблюдаемой $\mathbf{v}\sigma$ для кубита A в состоянии $|1\rangle$ означает проекционное измерение в базисе из векторов $|a\rangle$ и $|b\rangle$, то результат этого измерения равен «1» с вероятностью $P_A(1) = \frac{k_a^2}{4} = \frac{1-v_3}{2}$ или (−1) с вероятностью $P_A(-1) = \frac{1+v_3}{2}$.

Следовательно, пункт 3 утверждения доказан.

4. Первая часть данного пункта, касающаяся первого измерения над кубитом A, совпадает с первой частью пункта 3. Пусть в результате этого измерения получено значение «1». Тогда из пункта 3 данного утверждения следует, что при последующем измерении наблюдаемой $\mathbf{v}\sigma$ для кубита A результат равен «1» или «−1» соответственно с вероятностями $P_A(1) = \frac{1+v_3}{2}$, $P_A(-1) = \frac{1-v_3}{2}$.

В этом случае путем проведения соответствующих вычислений убеждаемся в том, что система равенств $\begin{cases} P_A(1) = 0{,}5, \\ P_A(-1) = 0{,}5 \end{cases}$ выполняется тогда и только тогда, когда $v_3 = 0$.

Аналогично, пусть в результате первого измерения получено значение «−1». Тогда из пункта 3 данного утверждения следует, что при последующем измерении наблюдаемой $\mathbf{v}\sigma$ для кубита A результат равен «1» или «−1» соответственно с вероятностями $P_A(1) = \frac{1-v_3}{2}$, $P_A(-1) = \frac{1+v_3}{2}$.

В этом случае непосредственной проверкой убеждаемся, что система равенств $\begin{cases} P_A(1) = 0,5, \\ P_A(-1) = 0,5 \end{cases}$ выполняется тогда и только тогда, когда $v_3 = 0$.

У т в е р ж д е н и е п о л н о с т ь ю д о к а з а н о .

2. Протокол квантовой криптографичесуой системы АКМ2017

Пусть сгенерировано достаточное число $N \in \mathbb{N}$ пар кубитов A_iB_i (где $i = \overline{1,N}$) в состоянии Белла $|\psi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$, называемом (по историческим причинам) *спиновым синглетом* [16], где $\mathbb{N}$ – множество натуральных чисел. Кубиты массива пар $\{A_iB_i \mid i = \overline{1,N}\}$ разделены так, что массив кубитов $\{A_i \mid i = \overline{1,N}\}$ составляет исходящий шифр-блокнот Алисы, а массив кубитов $\{B_i \mid i = \overline{1,N}\}$ составляет входящий шифр-блокнот Боба. Алиса и Боб разделены в пространстве, то есть, проще говоря, живут далеко друг от друга. *Может ли быть решена следующая задача?*

З а д а ч а . Алиса должна передать Бобу сообщение, имеющее в двоичном виде представление $m = m_1, m_2, \ldots, m_L$, длины $L \le N$ бит, зашифровав его с использованием своего исходящего блокнота, а Боб должен получить и расшифровать сообщение с использованием своего входящего блокнота. При этом предполагается, что Алиса и Боб располагают дополнительно еще общедоступным (открытым) классическим каналом связи.

О т в е т к поставленному вопросу: *да*. Для подтверждения истинности этого ответа изложим решение сформулированной задачи.

Р е ш е н и е . Пусть Алиса выбирает случайным образом (например, используя подходящий генератор случайных чисел) единичный вектор $\mathbf{v} = (v_1, v_2, v_3)$ (то есть вектор $\mathbf{v}$ является нормированным вектором [16]) в трехмерном пространстве над полем действительных чисел $\mathbb{R}$. Вектор $\mathbf{v}$ является *сеансовым (разовым) ключом* и используется для зашифрования только *одного* данного сообщения. Вектор $\mathbf{v}$ будет передан Бобу после завершения процесса зашифрования сообщения m вместе с зашифрованным сообщением (например, по предварительной договоренности в начале криптограммы перед зашифрованным сообщением) по классическому каналу. Будем полагать, что Алиса осуществляет зашифрование сообщения m последовательно по одному биту.

Для зашифрования двоичного символа m_i, где $i = \overline{1,L}$, Алиса осуществляет следующие действия:

1) выполняет измерение наблюдаемой $\mathbf{v}\sigma$ для кубита A_i и в зависимости от результата измерения «1» или «−1» полагает значение i-го знака γ_i двоичной гаммы $\gamma = \gamma_1, \gamma_2, \ldots, \gamma_L$ равным 0 или 1 соответственно;

2) вычисляет значение i-го знака s_i криптограммы (зашифрованного сообщения) $s = s_1, s_2, \ldots, s_L$ через равенство $s_i = m_i \oplus \gamma_i$, где $\oplus$ – знак операции сложения по модулю 2, $i = \overline{1,L}$;

3) выполняет измерение наблюдаемой $\sigma_3 = \sigma_{\mathbf{Z}} = \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ для кубита A_i и получает результат измерения «1» или «−1»; если получен результат «1», то кубит A_i оставляется в том состоянии (то есть в состоянии $|0\rangle$), в котором он оказался после измерения; если же получен результат «−1» (то есть состояние кубита A_i после измерения $-|1\rangle$), то к кубиту A_i применяется элемент $\sigma_1 = \sigma_{\mathbf{X}} = \mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, после чего он окажется в состоянии $|0\rangle$.

Возможно распараллеливание процесса зашифрования без ограничений, так как биты сообщения m зашифровываются независимо.

После завершения зашифрования сообщения m Алиса передает Бобу пару $(\mathbf{v}, s)$ (то есть криптограмму) по открытому классическому каналу связи.

Получив криптограмму $(\mathbf{v}, s)$, Боб выполняет процедуру расшифрования. Для расшифрования двоичного символа s_i, где $i = \overline{1, L}$, Боб осуществляет следующие действия:

1) выполняет измерение наблюдаемой $\mathbf{v}\sigma$ для кубита B_i и получает результат измерения «1» или «−1», противоположный в соответствии с пунктом 1 утверждения из предыдущего раздела с результатом, полученным Алисой при зашифровании знака m_i; далее Боб, в зависимости от полученного результата измерения «1» или «−1», полагает значение i-го знака γ_i двоичной гаммы $\gamma = \gamma_1, \gamma_2, \ldots, \gamma_L$ равным 1 или 0 соответственно (напомним, что у Алисы знак гаммы был равен 0 при получении результата ее измерения «1», а при результате измерения «−1» знак гаммы был равен 1);

2) вычисляет значение i-го знака m_i сообщения $m = m_1, m_2, \ldots, m_L$ через равенство $m_i = s_i \oplus \gamma_i$;

3) выполняет измерение наблюдаемой $\sigma_3 = \sigma_{\mathbf{Z}} = \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ для кубита B_i и получает результат измерения «1» или «−1»; если получен результат «1», то кубит B_i оставляется в том состоянии (то есть в состоянии $|0\rangle$), в котором он оказался после измерения; если же получен результат «−1» (то есть состояние кубита B_i после измерения $-|1\rangle$), то к кубиту B_i применяется элемент $\sigma_1 = \sigma_{\mathbf{X}} = \mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, после чего он окажется в состоянии $|0\rangle$.

Возможно распараллеливание процесса расшифрования без ограничений, так как биты сообщения m расшифровываются независимо.

Таким образом, в изложенном описании квантовой криптографической системы использовалось то, что *знаки двоичных гамм, сформированных и Алисой, и Бобом, совпадают*. Это следует из пункта 1 утверждения из предыдущего раздела.

Описанная квантовая криптографическая система получила название АКМ2017.

3. Сравнительный анализ АКМ2017 с известными криптографическими системами

Зададимся вопросом – каковы преимущества новой квантовой криптографической системы АКМ2017 по сравнению с известными классическими и квантовыми криптографическими системами?

Вначале изложим преимущества АКМ2017 по сравнению с известными квантовыми криптографическими системами, такими как BB84, E91, B92, SARG и т.д. [6, 10]:

1) исключена процедура определения значения гаммы путем проведения измерений (детектирования) в разных случайным образом выбираемых базисах, что исключает необходимость дополнительной передачи информации о выбранных базисах измерений (детекторах) по открытому классическому каналу связи;

2) для АКМ2017 ключевой материал (гамма) не накапливается у абонентов, а формируется при проведении процессов зашифрования и расшифрования;

3) у АКМ2017 более экономичный расход ключевого материала в том смысле, что для генерации n знаков гаммы в известных квантовых криптографических системах необходимо передать с помощью квантового канала в среднем от $2n$ посылок (фотонов или других частиц) каждому абоненту; этот показатель обеспечения ключевыми носителями в случае АКМ2017 в два раза меньше и режим обеспечения ключевыми носителями имеет принципиальные отличия;

4) для квантовой криптографической системы АКМ2017 существует принципиальная возможность с использованием операции *свопинг* (подкачка) провести дистанционную (например, используя космические спутники связи, аналогичные известным китайским спутникам квантовой связи [12]) регенерацию несепарабельных состояний (спиновых синглетов) использованных пар кубитов и, тем самым, повысить надежность шифрованной связи; для известных квантовых криптографических систем такая возможность отсутствует;

5) более высокий уровень стойкости при компрометации ключевых носителей.

Теперь обратимся к преимуществам квантовой криптографической системы АКМ2017 по сравнению с классическими криптографическими системами.

Сравнивать АКМ2017 с асимметричными криптографическими системами или с симметричными криптографическими системами с ограниченным ключом (не являющимися теоретически стойкими) не имеет смысла. Это обусловлено тем, что АКМ2017 является совершенной криптографической системой [2, 7, 18]. А перечисленные криптографические системы не являются совершенными шифрами [2, 7, 18], что влечет их уязвимость, например, при «силовой» атаке типа «тотальный перебор ключа», который реален, как предполагают, при применении в целях дешифрования квантовых компьютеров [9, 12].

Совершенность [2, 3, 7, 18] криптографической системы АКМ2017 следует из того, что по сути это совершенная криптографическая система «одноразовый шифр-блокнот» (криптографическая система Вернама) [18, 19] с улучшенными шифровальными блокнотами на основе использования квантового ресурса несепарабельности двухкубитного состояния спиновой синглет. Эти улучшения влекут за собой принципиально новые полезные качества, отсутствующие у криптографической системы «одноразовый шифр-блокнот». Прежде чем обсудить эти новые качества, приведем краткое описание криптографической системы «одноразовый шифр-блокнот» [2, 3, 7, 18, 19].

Алгоритм шифрования Вернама (то есть криптографическая система «одноразовый шифр-блокнот») заключается в том, что представленная в двоичном виде последовательность открытого текста побитово складывается по модулю 2 с ключом (называемым гаммой в российской криптографической литературе) – случайной двоичной последовательностью. Случайный набор символов ключа, написанных на листах бумаги и сброшюрованных в виде блокнота, используется только один раз и только для зашифрования одного сообщения. Отсюда, очевидно, и название шифра – «одноразовый шифр-блокнот». Закончив шифровать сообщение, отправитель уничтожает использованные страницы блокнота. В свою очередь, получатель, используя другой точно такой же блокнот, осуществляет расшифрование. Расшифровав сообщение, он уничтожает соответствующие страницы блокнота. Итак, для зашифрования каждого нового сообщения используются новые двоичные символы ключа и их число совпадает с длиной шифруемого сообщения.

Вернам не представил строгих доказательств того, что предложенный им шифр обладает высокими криптографическими качествами. Строгое математическое обоснование теоретической стойкости шифра Вернама осуществил К. Шеннон, опубликовавший в 1949 г. основные положения теоретической криптографии [18].

Заметим, что перехват сообщения, зашифрованного с помощью шифра «одноразовый шифр-блокнот», не содержит для криптоаналитика противника никакой информации, если ключ ему неизвестен и этот ключ обладает хорошими вероятностно-статистическими качествами (то есть является, в определенном смысле, совершенно случайным). Кроме этого, как было сказано ранее, число двоичных символов ключа, используемых для шифрования сообщения, совпадает с длиной шифруемого сообщения. Это означает, что использование шифра «одноразовый шифр-блокнот» для защиты больших объемов информации требует огромных издержек, связанных с производством, распределением, хранением и уничтожением ключевых материалов. Таким образом, критичной для практических применений компонентой шифра «одноразовый шифр-блокнот» является его система управления ключевой информацией, под которой понимается система, включающая в себя производство, распределение, хранение, использование и уничтожение ключевых материалов [2, 19].

Кроме того, компрометация шифровальных блокнотов приводит к несанкционированному полному доступу к защищаемой информации. То есть при компрометации шифровальных блокнотов стойкость криптографической системы «одноразовый шифр-блокнот» – нулевая (образно говоря), а в случае криптографической системы АКМ2017 ситуация намного лучше. Это одно из принципиальных новых преимуществ, присущих АКМ2017. Есть и другие. Не претендуя на исчерпывающую полноту, укажем на следующие *преимущества криптографической системы АКМ2017* по сравнению с классической криптографической системой «одноразовый шифр-блокнот»:

1) в случае АКМ2017 ключевая последовательность (гамма) генерируется на основе фундаментально случайного процесса, основанного на свойствах квантового ресурса несепарабельности двухкубитного состояния спиновой синглет – здесь, как говорит известный физик Жизан, «истинная» случайность

[6]; а в случае криптографической системы «одноразовый шифр-блокнот» используются методы формирования шифровальных блокнотов, основанные на классических подходах к исследованию случайных процессов [4, 5, 13];

2) в случае АКМ2017 появляется еще одна степень усиления стойкости, отсутствующая в случае криптографической системы «одноразовый шифр-блокнот» – это сеансовый ключ в виде единичного вектора $\mathbf{v} = (v_1, v_2, v_3)$ в трехмерном пространстве над полем действительных чисел $\mathbb{R}$; эта степень усиления стойкости выражается в следующем: при компрометации ключевых блокнотов стойкость криптографической системой «одноразовый шифр-блокнот» становится, образно говоря, нулевой; а в случае АКМ2017 ситуация более благоприятная в том плане, что стойкость в определенном смысле сохраняется;

3) для квантовой криптографической системы АКМ2017 существует принципиальная возможность с использованием операции *свопинг* (подкачка) [10] провести дистанционное установление носителей-кубитов использованных квантовых шифровальных блокнотов в состояние, пригодное для повторного использования данных квантовых шифровальных блокнотов и, тем самым, повысить надежность шифрованной связи; а для криптографической системы «одноразовый шифр-блокнот» такая возможность отсутствует.

Остановимся более подробно на пункте 1 (пункт 2 можно обосновать, используя утверждение из первого раздела; пункт 3 обоснован в [15]).

Итак, в случае АКМ2017 ключевая последовательность (гамма) генерируется на основе фундаментально случайного процесса, основанного на свойствах квантового ресурса несепарабельности двухкубитного состояния спиновой синглет. В случае же криптографической системы «одноразовый шифр-блокнот» используются методы формирования шифровальных блокнотов, основанные на классических подходах к исследованию случайных процессов. Считается, что ключевой материал, представленный в таких шифровальных блокнотах, по своим криптографическим качествам уступает ключевому материалу, сгенерированному на основе квантовых носителей «истинной» случайности (таких, например, как состояния Белла и, в частности, спиновой синглет). Попробуем разобраться в этих вопросах, следуя [6].

В классической физике считается, что результат любого измерения предопределен, что он в известном смысле записан в физическом состоянии системы, подвергающейся измерению [8, 14, 17]. Вероятности «появляются» только из-за того, что экспериментатору (наблюдателю и т.п., то есть субъекту, проводящему измерение) *точное физическое состояние неизвестно*. Это незнание приводит к необходимости использовать статистические методы и вероятностный расчет в соответствии с аксиомами Колмогорова [4, 5, 13]. Поясним сказанное на примере игры «орел или решка» с подбрасываемой монетой. Сложность микроявлений, например, удары об монету молекул воздуха или недостаточная точность сведений о неровности самой монеты и т.п., влечет невозможность предсказать однозначно результат (орел или решка) при подбрасывании монеты, что трактуется как случайность значения результата. Но эта невозможность не заложена в природе вещей: по сути она является следствием множества причин, неизвестных экспериментатору (в данном случае игроку) и составляющих его субъективное незнание, но реально существующих, сочетание которых и предопределяет конечный результат. Если бы экспериментатор (игрок) смог отследить детали движения монеты с надлежащей точностью и с адекватными средствами расчета, то, имея начальные условия броска, состояние молекул воздуха, уровень неровности монеты и т.п., он смог бы точно предсказать, какой стороной упадет монета. Поэтому возникающая при подбрасывании монеты случайность в результате (какой стороной упадет монета) является не истинной случайностью, а кажущейся случайностью, связанной с субъективным незнанием экспериментатора (игрока).

После разбора такого достаточно простого примера с монетой будет несложно понять, что и случайность, используемая при формирования шифровальных блокнотов в классической криптографической системе Вернама «одноразовый шифр-блокнот», не является истинной. Она является, в известной степени, кажущейся случайностью. Действительно, в этом случае шифровальные блокноты формируются на основе физических датчиков или путем использования псевдослучайных последовательностей, генерируемых компьютерами, или сочетанием данных способов. Случайность, порождаемая физическими датчиками, несмотря на все ухищрения, связанные со сложностью процесса, имеет ту же природу, что и случайность результатов при подбрасывании монеты, поэтому не является истинной. Что касается

псевдослучайных последовательностей, генерируемых компьютерами, то здесь генерируемые числовые последовательности таковы, что отношение между одним псевдослучайным числом и следующим заранее предопределено соответствующим правилом (полное отсутствие случайности), которое достаточно сложно для того, чтобы его можно было предугадать.

В квантовой физике результат измерения не предопределен никаким субъективным фактором, даже если *точное физическое состояние вполне известно*. В физическом состоянии системы, над которой производится измерение, записана лишь «предрасположенность» (более точно амплитуда) к проявлению того или иного возможного результата измерения. Эта предрасположенность не удовлетворяет [6] вероятностным аксиомам Колмогорова [4, 5, 13]. Вероятность каждого из двух значений результата первого однокубитного измерения над каждой квантовой системой из двух кубитов в состоянии спиновой синглет, составляющих в совокупности два массива (исходящий и входящий шифр-блокнот криптографической системы АКМ2017), должна быть равна 0,5. И возможные отклонения никак не связаны с отсутствием субъективных знаний о природе процесса, а определяются лишь точностью приборов, применяемых как для формирования и хранения двухкубитных квантовых систем в состоянии спиновой синглет в виде двух разных массивов (исходящий и входящий шифр-блокноты), так и для измерения. Если даже допустить, что применяемые приборы идеальны, все равно результат измерения случаен и ничем не предопределен. Невозможно убрать случайность путем совершенствования приборов [6].

Истинность случайности ключевого материала в квантовой криптографической системе АКМ2017 объясняется, прежде всего, отсутствием «даже в принципе» субъективного фактора – неполноты знаний о задействованных процессах. Деструктивное влияние этого субъективного фактора в классической физике допускается как наличие случайности (не истинной случайности), которую можно нивелировать путем устранения неполноты необходимых знаний [6].

- Квантовая криптографическая система АКМ2017 является новым представителем семейства криптографических систем защиты информации в системах высокой доступности, не теряющего своей актуальности с появлением квантового компьютера, то есть семейства криптографических систем, относящихся к так называемой постквантовой криптографии.

Литература

1. *Алиев Ф.К.*, *Корольков А.В.*, *Матвеев Е.А.* Несепарабельные состояния многокубитных квантовых систем. Монография / Под ред. *Ф.К. Алиева*. М.: Радиотехника. 2017. 320 с.
2. *Алферов А.П.*, *Зубов А.Ю.*, *Кузьмин А.С.*, *Черемушкин А.В.* Основы криптографии: Учеб. пособие. М.: Гелиос АРВ. 2005. 480 с.
3. *Бабаш А.В.*, *Шанкин Г.П.* Криптография. М.: СОЛОН-Р. 2002. 512 с.
4. *Боровков А.А.* Теория вероятностей. М.: Наука. 1976. 352 с.
5. *Боровков А.А.* Математическая статистика. М.: Наука. 1984. 472 с.
6. *Жизан Н.* Квантовая случайность. Пер. с англ. М.: Альпина нон-фикшн. 2016. 202 с.
7. *Зубов А.Ю.* Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ. 2005. 192 с.
8. *Иванов М.Г.* Как понимать квантовую механику. М.-Ижевск: НИЦ «Регулярная и хаотическая динамика». 2012. 516 с.
9. Квантовый компьютер. [Электронный ресурс]. URL = ru.wikipedia.org.
10. *Килин С.Я. и др.* Квантовая криптография: идеи и практика. Минск: Белорус. наука. 2007. 391 с.
11. Китайский спутник Мо Цзы. [Электронный ресурс]. URL = yandex.ru.
12. *Кокин А.А.* Твердотельные квантовые компьютеры на ядерных спинах. М.-Ижевск: Институт компьютерных исследований. 2004. 204 с.
13. *Коралов Л.Б.*, *Синай Я.Г.* Теория вероятностей и случайные процессы. М.: МЦНМО. 2013. 408 с.
14. *Матвеев А.Н.* Атомная физика: Учеб. пособие для вузов. М.: Изд-во «Мир и Образование». 2007. 432 с.
15. *Матвеев Е.А.* Протокол восстановления состояний носителей-кубитов для формирования ключевой информации квантовой криптографической системы АКМ2017 // Системы высокой доступности. 2018. № 4. С. 73−78.
16. *Нильсен М.*, *Чанг И.* Квантовые вычисления и квантовая информация. М.: Мир. 2006. 823 с.
17. *Фейнман Ричард Ф.*, *Лейтон Роберт Б.*, *Сэндс Мэтью* Фейнмановские лекции по физике: № 8, 9. Квантовая механика: Учеб. пособие. М.: Изд-во ЛКИ. 2008. 528 с.
18. *Шеннон К.* Работы по теории информации и кибернетике. М.: ИЛ. 1963. 869 с.
19. *Шнаер Б.* Прикладная криптография. М.: ТРИУМФ. 2003. 816 с.

Поступила 18 сентября 2018 г.

Quantum cryptographic system AKM2017 based on the inseparability of the spin singlet state

F.K. Aliev – Dr.Sc.(Phys.-Math.), Leading Adviser, Defense Ministry of RF
A.V. Korolkov – Ph.D.(Eng.), Associate Professor, Corresponding Member of Russian Cryptography Academy, Head of Department, RTU MIREA (Moscow); Head of Laboratory, Russian Cryptography Academy
E.A. Matveev – Director of «Cryptosoft» (Penza)
S.S. Orlov – Employee, Publishing House TVP (Moscow)
I.A. Sheremet – Corresponding Member of RAS, Dr.Sc.(Eng.), Professor, Deputy Director of RFBR (Moscow)

The possible emergence of quantum information processing technologies and quantum computing devices widely advertised in recent years can make significant adjustments to the existing situation in the field of information security, both in Russia and around the world. Forecast a multiple increase in the number of both imaginary and real threats. It is believed that the emergence of a «full-fledged quantum computer» will negate the possibility of ensuring information security by using asymmetric cryptographic systems and symmetric cryptographic systems with a limited key length that are not theoretically stable. Such a development of events may lead to a significant reduction in the fleet of cryptographic technology, suitable for practical applications.
This indicates the relevance of the development and application of new information protection mechanisms that are resistant to both currently known threats, and those that are caused by the alleged emergence of quantum computing devices. One of the promising ways in this direction can be the development and wide application of new information protection mechanisms based on quantum resources, including those that have no analogues in classical physics. Among a certain part of experts in the field of information security, even the opinion is widespread that the forthcoming quantum technologies give more advantages to information protection than actions to overcome it. It may well be that new mechanisms can withstand the computational power of quantum computers with efficiency no less than theoretically persistent classical cryptographic systems, and, at the same time, lack their shortcomings hindering full-fledged widespread practical use. We believe that the results presented in this article can serve to support these theses.
The article presents the main provisions of the new quantum cryptographic system AKM2017, based on the use of the quantum resource of non-separability of the spin singlet state. The results of a comparative analysis of AKM2017 with respect to classical cryptographic systems and known quantum cryptographic systems are presented.
The article consists of the introduction of three sections.
The first section of the article is devoted to the identification and description of the properties of such a resource of quantum physics as a resource of non-separability of the state of a quantum system of two qubits known as the spin singlet. The corresponding assertion is formulated and proved.
The second section of the article presents the protocol of the quantum cryptographic system AKM2017. The protocol is based on the statement about the properties of the spin singlet state, presented with the proof in the first section of the article.
Last section 3 devoted to comparative analyses of AKM2017 with known cryptographic systems.
Attention is focused on the new qualitative properties of the quantum cryptographic system AKM2017. The aggregate of these properties is impossible in principle for both classical cryptographic systems and (in the sense of all its exhaustive completeness) for the previously known systems of quantum cryptography.

References

1. *Aliev F.K.*, *Korol'kov A.V.*, *Matveev E.A.* Neseparabel'ny'e sostoyaniya mnogokubitny'x kvantovy'x sistem. Monografiya / Pod red. *F.K. Alieva*. M.: Radiotexnika. 2017. 320 s.
2. *Alferov A.P.*, *Zubov A.Yu.*, *Kuz'min A.S.*, *Cheremushkin A.V.* Osnovy' kriptografii: Ucheb. posobie. M.: Gelios ARV. 2005. 480 s.
3. *Babash A.V.*, *Shankin G.P.* Kriptografiya. M.: SOLON-R. 2002. 512 s.
4. *Borovkov A.A.* Teoriya veroyatnostej. M.: Nauka. 1976. 352 s.
5. *Borovkov A.A.* Matematicheskaya statistika. M.: Nauka. 1984. 472 s.
6. *Zhizan N.* Kvantovaya sluchajnost'. Per. s angl. M.: Al'pina non-fikshn. 2016. 202 s.
7. *Zubov A.Yu.* Kriptograficheskie metody' zashhity' informaczii. Sovershenny'e shifry'. M.: Gelios ARV. 2005. 192 s.
8. *Ivanov M.G.* Kak ponimat' kvantovuyu mexaniku. M.-Izhevsk: NICz «Regulyarnaya i xaoticheskaya dinamika». 2012. 516 s.
9. Kvantovy'j komp'yuter. [E'lektronny'j resurs]. URL = ru.wikipedia.org.
10. *Kilin S.Ya. i dr.* Kvantovaya kriptografiya: idei i praktika. Minsk: Belorus. nauka. 2007. 391 s.
11. Kitajskij sputnik Mo Czzy'. [E'lektronny'j resurs]. URL = yandex.ru.
12. *Kokin A.A.* Tverdotel'ny'e kvantovy'e komp'yutery' na yaderny'x spinax. M.-Izhevsk: Institut komp'yuterny'x issledovanij. 2004. 204 s.
13. *Koralov L.B.*, *Sinaj Ya.G.* Teoriya veroyatnostej i sluchajny'e proczessy'. M.: MCzNMO. 2013. 408 s.
14. *Matveev A.N.* Atomnaya fizika: Ucheb. posobie dlya vuzov. M.: Izd-vo «Mir i Obrazovanie». 2007. 432 s.
15. *Matveev E.A.* Protokol vosstanovleniya sostoyanij nositelej-kubitov dlya formirovaniya klyuchevoj informaczii kvantovoj kriptograficheskoj sistemy' AKM2017 // Sistemy' vy'sokoj dostupnosti. 2018. № 4. S. 73–78.
16. *Nil'sen M.*, *Chang I.* Kvantovy'e vy'chisleniya i kvantovaya informacziya. M.: Mir. 2006. 823 s.
17. *Fejnman Richard F.*, *Lejton Robert B.*, *Se'nds Me't'yu* Fejnmanovskie lekczii po fizike: № 8, 9. Kvantovaya mexanika: Ucheb. posobie. M.: Izd-vo LKI. 2008. 528 s.
18. *Shennon K.* Raboty' po teorii informaczii i kibernetike. M.: IL. 1963. 869 s.
19. *Shnaer B.* Prikladnaya kriptografiya. M.: TRIUMF. 2003. 816 s.

УДК 004.056.55

Протокол восстановления состояний носителей-кубитов для формирования ключевой информации квантовой криптографической системы АКМ2017

Е.А. Матвеев – директор НТП «Криптософт» (г. Пенза)

Представлены основные положения протокола восстановления состояний носителей-кубитов ключевой информации для новой квантовой криптографической системы АКМ2017. Показано, что протокол реализует идею дистанционного формирования состояния спиновой синглет двухкубитной квантовой системы. Отмечено, что выполнение этого протокола гарантирует возможность многократного безопасного использования одних и тех же ключевых носителей, что позволяет повысить устойчивость связи в системах высокой доступности, в которых для защиты информации используется квантовая криптографическая система АКМ2017.

Ключевые слова: *протокол, квантовая криптография, криптографическая система, кубит, квантовая система, состояние спиновой синглет, перенос перепутывания – «свопинг», системы высокой доступности.*

The article presents the main provisions of the protocol for restoring the states-carriers of qubits of key information for the new quantum cryptographic system AKM2017. The protocol realizes the idea of the remote formation of the spin singlet state of a two-qubit quantum system. The implementation of this protocol ensures the possibility of multiple safe use of the same key carriers. This makes it possible to increase the stability of communication in highly available systems, in which the quantum cryptographic system AKM2017 is used to protect information.

Keywords: *protocol, quantum cryptography, cryptographic system, qubit, quantum system, spin singlet state, transfer of entanglement – «swapping», highly available systems.*

DOI: 10.18127/j20729472-201804-12

Ц е л ь р а б о т ы – представить основные положения протокола восстановления состояний носителей-кубитов ключевой информации для новой квантовой криптографической системы АКМ2017.

Из описания криптографической системы АКМ2017, представленного в [1], следует, что носители-кубиты для формирования ключевой информации после их использования не уничтожаются, а в обязательном порядке устанавливаются в состояние $|0\rangle$. Возникает вопрос – существует ли принципиальная возможность их восстановления в состояние, пригодное для повторного использования? *Ответ положительный*.

Восстановление пар носителей-кубитов для формирования ключевой информации в состоянии спиновой синглет $|\psi_{11}\rangle = \dfrac{|01\rangle - |10\rangle}{\sqrt{2}}$ [3] можно осуществить дистанционно с использованием внешнего источника пар запутанных фотонов в состоянии спиновой синглет $|\psi_{11}\rangle$ (например, с использованием спутников, подобных тем, что построены в китайско-европейском проекте 2013−2017 гг.) с помощью процедуры, близкой к процедуре «свопинг» – перенос перепутывания [2].

Обратим внимание на обозначение $|\kappa_1\kappa_2\cdots\kappa_r\rangle$:

$$|\kappa_1\kappa_2\cdots\kappa_r\rangle = |\kappa_1\rangle\,|\kappa_2\rangle\ \ldots\ |\kappa_r\rangle = |\kappa_1\rangle\otimes|\kappa_2\rangle\otimes\ \ldots\ \otimes|\kappa_r\rangle,$$

где $\kappa_1, \kappa_2, \ldots, \kappa_r \in \{0, 1\}$; $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$; $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$; r – произвольное натуральное число; $\otimes$ – знак тензорного произведения [1, 3].

Протокол процедуры восстановления состоит из двух частей, и для одной использованной пары носителей-кубитов A и B в состоянии $|0\rangle$ он выглядит следующим образом.

Часть 1. Вначале у Алисы и у Боба два кубита A и B, каждый из которых находится в состоянии $|0\rangle$.

Алиса и Боб удалены в пространстве друг от друга и они самостоятельно и заблаговременно, используя по одному дополнительному кубиту A_1 и B_1 также в состоянии $|0\rangle$, создают соответственно пары A_1A (пара кубитов Алисы) и B_1B (пара кубитов Боба), каждая из которых находится в состоянии Белла $|\psi_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$.

Изложим *соответствующий пошаговый алгоритм действий на примере Алисы.* На входе алгоритма два кубита A_1A в состоянии $|\psi_0^{(2)}\rangle = |00\rangle$.

Ш а г 1 . Алиса пропускает кубит A_1 через элемент Адамара **H** [3], что равносильно применению к состоянию $|\psi_0^{(2)}\rangle$ линейного преобразования с матрицей $\mathbf{H}\otimes\mathbf{I}_2$, где $\mathbf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$; $\mathbf{I}_2 = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$; $\otimes$ – знак тензорного произведения. В результате квантовая система A_1A переходит в состояние $|\psi_1^{(2)}\rangle$, задаваемое равенством $|\psi_1^{(2)}\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}|0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}$.

Ш а г 2 . Алиса пропускает свои кубиты A_1 и A через элемент **CNOT** [3]. Это равносильно тому, что к состоянию $|\psi_1^{(2)}\rangle$ применяется линейное преобразование с матрицей $\mathbf{CNOT}\otimes\mathbf{I}_2$, где

$$\mathbf{CNOT} = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}.$$

В результате получается состояние $|\psi_2^{(2)}\rangle$ квантовой системы A_1A, задаваемое равенством $|\psi_2^{(2)}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\psi_{00}\rangle$.

Аналогично, Боб также создает пару кубитов B_1B в состоянии $|\psi_2^{(2)}\rangle = |\psi_{00}\rangle$.

Часть 2. Внешний источник генерирует два кубита A_2B_2 в состоянии Белла спиновой синглет $|\psi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$ и направляет кубит A_2 Алисе и кубит B_2 Бобу.

Изложим *соответствующий пошаговый алгоритм действий вначале на примере Алисы, а затем на примере Боба*. Не имеет принципиального значения очередность действий Алисы и Боба. Для определенности положим, что Алиса действует первой. На входе алгоритма четыре кубита $B_2A_2A_1A$ в состоянии $|\psi_0^{(4)}\rangle = \frac{|10\rangle - |01\rangle}{\sqrt{2}}\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{1}{2}(|1000\rangle + |1011\rangle - |0100\rangle - |0111\rangle)$.

Ш а г 1 . Алиса пропускает свои кубиты A_2 и A_1 через элемент **CNOT** [3]. Это равносильно тому, что к состоянию $|\psi_0^{(4)}\rangle$ применяется линейное преобразование с матрицей $\mathbf{I}_2\otimes\mathbf{CNOT}\otimes\mathbf{I}_2$. В результате получается состояние $|\psi_1^{(4)}\rangle$ квантовой системы $B_2A_2A_1A$, задаваемое равенством

$$|\psi_1^{(4)}\rangle = \frac{1}{2}(|1000\rangle + |1011\rangle - |0110\rangle - |0101\rangle).$$

Ш а г 2 . Алиса пропускает свой кубит A_2 через элемент Адамара **H** [3], что равносильно применению к состоянию $|\psi_1^{(4)}\rangle$ линейного преобразования с матрицей $\mathbf{I}_2\otimes\mathbf{H}\otimes\mathbf{I}_2\otimes\mathbf{I}_2$. В результате квантовая система $B_2A_2A_1A$, переходит в состояние $|\psi_2^{(4)}\rangle$, задаваемое равенством

$$\left|\psi_2^{(4)}\right\rangle = \frac{1}{2}\left(|1\rangle\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle|0\rangle + |1\rangle\frac{|0\rangle+|1\rangle}{\sqrt{2}}|1\rangle|1\rangle - |0\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}|1\rangle|0\rangle - |0\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}|0\rangle|1\rangle\right) =$$

$$= \frac{1}{2}\left[-\frac{1}{\sqrt{2}}\left(|0\rangle|00\rangle|1\rangle - |1\rangle|00\rangle|0\rangle\right) - \frac{1}{\sqrt{2}}\left(|0\rangle|01\rangle|0\rangle - |1\rangle|01\rangle|1\rangle\right) + \frac{1}{\sqrt{2}}\left(|0\rangle|10\rangle|1\rangle + |1\rangle|10\rangle|0\rangle\right) +\right.$$

$$\left. + \frac{1}{\sqrt{2}}\left(|0\rangle|11\rangle|0\rangle + |1\rangle|11\rangle|1\rangle\right)\right].$$

Ш а г 3 . Алиса проводит измерение над своими двумя кубитами A_2 и A_1 в вычислительном базисе из векторов $|00\rangle$, $|01\rangle$, $|10\rangle$ и $|11\rangle$ [3]. В результате этого измерения квантовая система из четырех кубитов $B_2A_2A_1A$ может иметь следующие свои состояния и состояния своих подсистем:

1) с вероятностью $\frac{1}{4}$ квантовая система $B_2A_2A_1A$ в состоянии $\frac{1}{\sqrt{2}}(|0\rangle|00\rangle|1\rangle - |1\rangle|00\rangle|0\rangle)$ и при этом подсистема из двух кубитов A_2A_1 в состоянии $|00\rangle$, а подсистема из двух кубитов B_2A в состоянии Белла спиновой синглет $|\psi_{11}\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$ (это следует из результатов, представленных в [1]; далее такая ссылка предполагается по умолчанию);

2) с вероятностью $\frac{1}{4}$ квантовая система $B_2A_2A_1A$ в состоянии $\frac{1}{\sqrt{2}}(|0\rangle|01\rangle|0\rangle - |1\rangle|01\rangle|1\rangle)$ и при этом подсистема из двух кубитов A_2A_1 в состоянии $|01\rangle$, а подсистема из двух кубитов B_2A в состоянии Белла $|\psi_{10}\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}}$;

3) с вероятностью $\frac{1}{4}$ квантовая система $B_2A_2A_1A$ в состоянии $\frac{1}{\sqrt{2}}(|0\rangle|10\rangle|1\rangle + |1\rangle|10\rangle|0\rangle)$ и при этом подсистема из двух кубитов A_2A_1 в состоянии $|10\rangle$, а подсистема из двух кубитов B_2A в состоянии Белла $|\psi_{01}\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$;

4) с вероятностью $\frac{1}{4}$ квантовая система $B_2A_2A_1A$ в состоянии $\frac{1}{\sqrt{2}}(|0\rangle|11\rangle|0\rangle + |1\rangle|11\rangle|1\rangle)$ и при этом подсистема из двух кубитов A_2A_1 в состоянии $|11\rangle$, а подсистема из двух кубитов B_2A в состоянии Белла $|\psi_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$.

Ш а г 4 . Если на шаге 3 в результате измерения Алисы два кубита A_2A_1 оказались в состоянии $|00\rangle$, то Алиса не делает ничего. Кубиты B_2A находятся в состоянии Белла спиновой синглет $|\psi_{11}\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$.

Если на шаге 3 в результате измерения Алисы два кубита A_2A_1 оказались в состоянии $|01\rangle$, то Алиса пропускает кубит A через элемент Паули $\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. В результате этого кубиты B_2A окажутся в состоянии Белла спиновой синглет $|\psi_{11}\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$.

Если на шаге 3 в результате измерения Алисы два кубита A_2A_1 оказались в состоянии $|10\rangle$, то Алиса пропускает кубит A через элемент Паули $\mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. В результате этого кубиты B_2A окажутся

с точностью до общего сомножителя (−1) в состоянии Белла спиновой синглет $|\psi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$.

Если на шаге 3 в результате измерения Алисы два кубита A_2A_1 оказались в состоянии $|11\rangle$, то Алиса пропускает кубит A сперва через элемент Паули $\mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, а затем через элемент Паули $\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. В результате кубиты B_2A окажутся с точностью до общего сомножителя (−1) в состоянии Белла спиновой синглет $|\psi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$.

Теперь изложим *соответствующий пошаговый алгоритм действий Боба*. На входе алгоритма четыре кубита AB_2B_1B в состоянии $|\psi_0^{(4)}\rangle = \frac{|10\rangle - |01\rangle}{\sqrt{2}} \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{1}{2}(|1000\rangle + |1011\rangle - |0100\rangle - |0111\rangle)$.

Ш а г 1 . Боб пропускает свои кубиты B_2 и B_1 через элемент **CNOT** [3]. Это равносильно тому, что к состоянию $|\psi_0^{(4)}\rangle$ применяется линейное преобразование с матрицей $\mathbf{I}_2 \otimes \mathbf{CNOT} \otimes \mathbf{I}_2$. В результате получается состояние $|\psi_1^{(4)}\rangle$ квантовой системы AB_2B_1B, задаваемое равенством

$$|\psi_1^{(4)}\rangle = \frac{1}{2}(|1000\rangle + |1011\rangle - |0110\rangle - |0101\rangle).$$

Ш а г 2 . Боб пропускает свой кубит B_2 через элемент Адамара **H** [3], что равносильно применению к состоянию $|\psi_1^{(4)}\rangle$ линейного преобразования с матрицей $\mathbf{I}_2 \otimes \mathbf{H} \otimes \mathbf{I}_2 \otimes \mathbf{I}_2$. В результате квантовая система AB_2B_1B, переходит в состояние $|\psi_2^{(4)}\rangle$, задаваемое равенством

$$|\psi_2^{(4)}\rangle = \frac{1}{2}\left(|1\rangle\frac{|0\rangle + |1\rangle}{\sqrt{2}}|0\rangle|0\rangle + |1\rangle\frac{|0\rangle + |1\rangle}{\sqrt{2}}|1\rangle|1\rangle - |0\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}}|1\rangle|0\rangle - |0\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}}|0\rangle|1\rangle\right) =$$

$$= \frac{1}{2}\left[-\frac{1}{\sqrt{2}}(|0\rangle|00\rangle|1\rangle - |1\rangle|00\rangle|0\rangle) - \frac{1}{\sqrt{2}}(|0\rangle|01\rangle|0\rangle - |1\rangle|01\rangle|1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle|10\rangle|1\rangle + |1\rangle|10\rangle|0\rangle) + \right.$$

$$\left. + \frac{1}{\sqrt{2}}(|0\rangle|11\rangle|0\rangle + |1\rangle|11\rangle|1\rangle)\right].$$

Ш а г 3 . Боб проводит измерение над своими двумя кубитами B_2 и B_1 в вычислительном базисе из векторов $|00\rangle$, $|01\rangle$, $|10\rangle$ и $|11\rangle$ [3]. В результате этого измерения квантовая система из четырех кубитов AB_2B_1B может иметь следующие свои состояния и состояния своих подсистем:

1) с вероятностью $\frac{1}{4}$ квантовая система AB_2B_1B в состоянии $\frac{1}{\sqrt{2}}(|0\rangle|00\rangle|1\rangle - |1\rangle|00\rangle|0\rangle)$ и при этом подсистема из двух кубитов B_2B_1 в состоянии $|00\rangle$, а подсистема из двух кубитов AB в состоянии Белла спиновой синглет $|\psi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$;

2) с вероятностью $\frac{1}{4}$ квантовая система AB_2B_1B в состоянии $\frac{1}{\sqrt{2}}(|0\rangle|01\rangle|0\rangle - |1\rangle|01\rangle|1\rangle)$ и при этом подсистема из двух кубитов B_2B_1 в состоянии $|01\rangle$, а подсистема из двух кубитов AB в состоянии Белла $|\psi_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$;

3) с вероятностью $\frac{1}{4}$ квантовая система AB_2B_1B в состоянии $\frac{1}{\sqrt{2}}(|0\rangle|10\rangle|1\rangle + |1\rangle|10\rangle|0\rangle)$ и при этом подсистема из двух кубитов B_2B_1 в состоянии $|10\rangle$, а подсистема из двух кубитов AB в состоянии Белла $|\psi_{01}\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$;

4) с вероятностью $\frac{1}{4}$ квантовая система AB_2B_1B в состоянии $\frac{1}{\sqrt{2}}(|0\rangle|11\rangle|0\rangle + |1\rangle|11\rangle|1\rangle)$ и при этом подсистема из двух кубитов B_2B_1 в состоянии $|11\rangle$, а подсистема из двух кубитов AB в состоянии Белла $|\psi_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$.

Ш а г 4. Если на шаге 3 в результате измерения Боба два кубита B_2B_1 оказались в состоянии $|00\rangle$, то Боб не делает ничего. Кубиты AB находятся в состоянии Белла спиновой синглет $|\psi_{11}\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$.

Если на шаге 3 в результате измерения Боба два кубита B_2B_1 оказались в состоянии $|01\rangle$, то Боб пропускает кубит B через элемент Паули $\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. В результате этого кубиты AB окажутся в состоянии Белла спиновой синглет $|\psi_{11}\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$.

Если на шаге 3 в результате измерения Боба два кубита B_2B_1 оказались в состоянии $|10\rangle$, то Боб пропускает кубит B через элемент Паули $\mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. В результате этого кубиты AB окажутся с точностью до общего сомножителя (−1) в состоянии Белла спиновой синглет $|\psi_{11}\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$.

Если на шаге 3 в результате измерения Боба два кубита B_2B_1 оказались в состоянии $|11\rangle$, то Боб пропускает кубит B сперва через элемент Паули $\mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, а затем через элемент Паули $\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. В результате этого кубиты AB окажутся с точностью до общего сомножителя (−1) в состоянии Белла спиновой синглет $|\psi_{11}\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$.

- При реализации разработанного квантового протокола квантовая система AB из кубитов Алисы и Боба соответственно установлена в необходимое состояние спиновой синглет и может быть использована для генерации одного бита ключа криптографической системы АКМ2017 для защиты информации в системах высокой доступности.

Литература

1. *Алиев Ф.К.*, *Корольков А.В.*, *Матвеев Е.А.*, *Орлов С.С.*, *Шеремет И.А.* Квантовая криптографическая система АКМ2017 на основе ресурса несепарабельности состояния спиновой синглет // Системы высокой доступности. 2018. № 4. С. 61–72.
2. *Килин С.Я. и др.* Квантовая криптография: идеи и практика. Минск: Белорусская наука. 2007. 391 с.
3. *Нильсен М.*, *Чанг И.* Квантовые вычисления и квантовая информация. М.: Мир. 2006. 824 с.

Поступила 18 сентября 2018 г.

The protocol of the recovery of carrier-qubit states for the formation of key information in the quantum cryptographic system AKM2017

E.A. Matveev – Director of «Cryptosoft» (Penza)

From the description of the cryptographic system AKM2017 it follows that the qubit carriers for the formation of key information after their use are not destroyed. The question arises: is there a principal possibility of their restoration in a state suitable for re-use?
The answer is yes. The recovery of carrier-qubit pairs for the formation of key information in the spin singlet state can be carried out remotely using an external source of pairs of entangled photons in the spin singlet state (for example, using satellites similar to those built in the Sino-European project of 2013–2017). using a procedure close to the «swapping» procedure – the transfer of entanglement. The article presents the main provisions of the protocol for restoring the states-carriers of qubits of key information for the new quantum cryptographic system AKM2017. The protocol realizes the idea of the remote formation of the spin singlet state of a two-qubit quantum system. The implementation of this protocol ensures the possibility of multiple safe use of the same key carriers. This makes it possible to increase the stability of communication in highly available systems, in which the quantum cryptographic system AKM2017 is used to protect information.

References

1. *Aliev F.K.*, *Korol'kov A.V.*, *Matveev E.A.*, *Orlov S.S.*, *Sheremet I.A.* Kvantovaya kriptograficheskaya sistema AKM2017 na osnove resursa neseparabel'nosti sostoyaniya spinovoj singlet // Sistemy' vy'sokoj dostupnosti. 2018. № 4. S. 61–72.
2. *Kilin S.Ya. i dr.* Kvantovaya kriptografiya: idei i praktika. Minsk: Belorusskaya nauka. 2007. 391 s.
3. *Nil'sen M.*, *Chang I.* Kvantovy'e vy'chisleniya i kvantovaya informacziya. M.: Mir. 2006. 824 s.