УДК 004.94:519.711.3

В. И. ПОТАПОВ
О. А. ГОРН

Омский государственный технический университет

МАТЕМАТИЧЕСКИЕ МОДЕЛИ И ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ КОМПЬЮТЕРНОЙ РЕАЛИЗАЦИИ ЗАДАЧ ОПТИМАЛЬНОГО УПРАВЛЕНИЯ ПРОТИВОБОРСТВУЮЩИМИ ПОДВИЖНЫМИ И НЕПОДВИЖНЫМИ ОБЪЕКТАМИ

Поставлена задача и разработана математическая модель противоборства двух избыточных технических систем, участвующих в конфликтной ситуации. Разработан программный комплекс для численного решения поставленной задачи на компьютере, которая сведена к дифференциальной игре между противоборствующими подвижными и неподвижными объектами и подвижными объектами.

Ключевые слова: математическая модель, противоборство, подвижные объекты, неподвижные объекты, дифференциальная игра, программный комплекс.

Введение. Будем рассматривать задачу, когда подвижная система, участвующая в конфликтной ситуации, в течение времени конфликта и положения в пространстве должна защищаться за счет собственных ресурсов — средств защиты (как правило — избыточности) от воздействия другой из участвующих в конфликте сторон, стремящейся своими средствами нападения увеличить вероятность отказа подвижного объекта в течение конфликта в пространстве взаимодействия, то есть уменьшить надежность подвижного объекта с системой его управления и надежность аппаратных компонентов подвижного объекта (подвижной системы).

Таким образом, в качестве причины отказа участвующего в конфликтной ситуации управляемого подвижного объекта являются отказы его аппаратных компонентов, отказы системы управления и особенности свойств пространства в котором перемещается управляемый объект, на которые оказывает соответствующее негативное влияние противоположная сторона, участвующая в конфликте.

Формализация объекта исследования и общая постановка задачи противоборства. Будем считать, что участвующий в конфликтной ситуации подвижный объект представляет собой перемещающуюся в трехмерном евклидовом пространстве R^3 избыточную $S_q(n, m, \bar{s}, q, \lambda(t, \bar{r}), \bar{\tau})$ — систему, состоящую из n основных модулей, разбитых на q групп по $n_1, n_2, ..., n_q$ $(n_i \geq 1)$ модулей в каждой. Интенсивности отказов модулей, входящих в соответствующую группу $\lambda_1(t, \bar{r}), \lambda_2(t, \bar{r}), ..., \lambda_q(t, \bar{r})$, являются функциями времени и точки пространства, в которой находится система. В состав подвижной системы входят, по числу основных q групп, резервные модули: по $s_1, s_2, ..., s_q$ $(s_i \geq 0)$ модулей в каждой группе $s_1+s_2+...+s_q = m$ интенсивность отказов каждого из которых также является функцией времени и точки пространства $\lambda_0(t, \bar{r})$. В каждой q-ой группе основные модули при их отказе мгновенно замещаются резервными из этой же группы. Как только резервный модуль подключается вместо отказавшего основного в своей группе, он начинает функционировать с интенсивностью отказов $\lambda_i(t, \bar{r}), (1 \leq i \leq q)$.

Считаем, что вектор резервирования $\bar{s}=(s_1, s_2, ..., s_q)$ является переменным во времени, т.е. в моменты времени $\tau_1, \tau_2, ..., \tau_l$ по командам может происходить перераспределение резервных модулей между группами, которое назовем настройкой системы, а соответствующие моменты времени $\tau_\sigma (1 \leq \sigma \leq L)$ — моментами настройки и, соответственно, $\bar{\tau}=(\tau_1, \tau_2, ..., \tau_\sigma)$ — вектором настройки. Каждому моменту настройки τ_σ соответствует вектор резервирования $\bar{s}_\sigma = (s_{\sigma 1}, s_{\sigma 2}, ..., s_{\sigma q})$. Количество настроек за время движения системы t_f ограничено L $(L \geq 0)$.

Рассматриваемая задача может быть формально сформулирована следующим образом.

При заданных $\lambda_{i\_}=\lambda_i(t, \bar{r}), (0 \leq i \leq q)$ для системы $S_q(n, m, \bar{s}, q, \lambda(t, \bar{r}), \bar{\tau})$, участвующей в конфликтной ситуации, разработать алгоритм оптимального управления, включающий алгоритмы вычисления траектории ее движения $\bar{r}=\bar{r}(t)$, вектора настройки $\{\tau_1, \tau_2, ..., \tau_L\}$ и векторов резервирования $\bar{s}_\sigma = (s_{\sigma 1}, s_{\sigma 2}, ..., s_{\sigma q})$, $(0 \leq y \leq L)$, отвечающих моментам настройки τ_σ, максимизирующих вероятность безотказной работы $P(t_f)$ подвижной конфликтующей системы в момент t_f прибытия ее в заданную точку $\bar{r}_f$ пространства. То есть решить задачу оптимизации выбора траектории и пространственно-временной стратегии резервирования избыточной подвижной системы, участвующей в конфликте, с целью мак-

симизации ее вероятности безотказной работы $P(t_f)$ при движении по выбранной траектории, включая конечную точку движения [1].

В приведенной выше постановке рассматриваемая задача сводится к задаче оптимального управления подвижной системой S_n, где (в терминах теории оптимального управления [2]) в качестве максимизирующего функционала качества управления является $P(t_f)$, в качестве управления используются $\bar{r}, \bar{\tau}, \bar{s}_\sigma$, в качестве внешнего воздействия на систему используются $\lambda_i = \lambda_i(t, \bar{r})$, при ограничениях $1 \le i \le q$, $0 \le y \le L$ и естественных ограничениях на параметры движения подвижной S_n-системы, которые приведены в [3].

Очевидно, что аналитическое решение поставленной задачи оптимального управления, участвующей в конфликтной ситуации подвижной S_n-системой, не представляется возможным, поэтому для решения задачи следует пользоваться приближенным численным методом, основанным на методе дискретизации, подробно рассмотренном в [4].

Суть этого метода, применительно к рассматриваемой задаче, состоит в том, что систему дифференциальных уравнений, описывающих поведения противоборствующей S_n-системы, коэффициенты которой являются функциями времени и точки пространства, в которой находится подвижная система, необходимо заменить системой дискретных аналогов, у которых коэффициенты можно рассматривать как постоянные (с заранее установленной степенью точности) на дискретных интервалах времени и пространства, в котором движется участвующая в конфликтной ситуации S_n-система.

Перейдем теперь к рассмотрению задач противоборства в конфликтной ситуации между подвижными и неподвижными объектами и между подвижными объектами, для решения которых разработан рассматриваемый в данной работе программный комплекс.

Противоборство (дифференциальная игра) между подвижными и неподвижными объектами. В данном разделе работы разработана математическая модель для решения игровой задачи типа «нападение-защита» для двух игроков, располагающих подвижными (нападающими) и неподвижными (защищающимися) объектами (системами) соответственно. При этом при приближении подвижного объекта к неподвижному на определенное расстояние противоборствующие системы начинают целенаправленно воздействовать друг на друга, увеличивая интенсивность отказов компонентов системы противника, то есть уменьшать функциональную надежность соответствующей противоборствующей системы [5].

Дифференциальная игра между противоборствующими объектами сведена к минимаксной игре в смешанных стратегиях с функцией выигрыша, равной разности сумм вероятностей безотказной работы объектов нападения и объектов защиты в течение времени игры. При этом множеством стратегий, для выбора из них оптимальной, для нападающего игрока является набор траекторий перемещения подвижных объектов к местам нападения, а множеством стратегий для защищающегося игрока, для выбора из них оптимальной, является целенаправленный выбор места расположения объектов защиты в заданной области расположения защищающихся — неподвижных объектов.

В соответствии со сказанным, рассмотрим следующую игру двух лиц. Игрок 1 располагает L управляемыми объектами, находящимися в начальных точках $\bar{r}_{k0}$, $1 \le k \le L$. Игрок 2 — N единицами защиты, которые он может расставлять в заданной области Γ, причем $\bar{r}_{k0} \in \Gamma$. Игрок 1 старается поразить k-м управляемым объектом $1 \le k \le L$ заданную точку $\bar{r}_{kf} \in \Gamma$, которую защищает игрок 2, а игрок 2 старается помешать этому. Обозначим через t_{kf} время полета k-ого объекта от точки $\bar{r}_{k0}$ до $\bar{r}_{kf}$. Число t_{kf} зависит от траектории $\bar{r}_k = \bar{r}_k(t)$, выбираемой k-м объектом, причем $r_k(0) = r_{k0}$, $r_k(t_f) = r_{kf}$.

Пусть, далее, множество пунктов защиты игрока 2 может быть расположено в Q точках ($N \le Q$) с заданными координатами $\bar{c}_i = (c_{1i}, c_{2i}, c_{3i})$, $1 \le i \le Q$. Обозначим множество $\{\bar{c}_1, \bar{c}_2, ..., \bar{c}_Q\}$ через C.

Итак, игроки 1 и 2, которые обладают каждый L $S_q[1, \lambda_{kq}(t, \bar{r}_k)]$ — системами соответственно ($q = 1, 2$), поведение которых, при аппроксимации марковским процессом, описывается дифференциальными уравнениями Колмагорова с переменными коэффициентами.

В качестве функции выигрыша возьмем

$$K[z_1, z_2] = \sum_{k=1}^{L} p_{k1}(t_{kf}) - \sum_{k=1}^{L} p_{k2}(t_{kf}), \qquad (1)$$

где $z_q \in W^q$, а W^q — множества стратегий q-го игрока ($q = 1, 2$).

Ясно, что

$$W^1 = \{r_1(t), r_2(t), ..., r_L(t)\}, \qquad (2)$$
$$W^2 = (\delta_1, \delta_2, ..., \delta_R),$$

где $R = \binom{Q}{N}$.

Решением задачи является вычисление стратегий $\tilde{z}_1$ и $\tilde{z}_2$, для которых

$$K[\tilde{z}_1, \tilde{z}_2] = \min_{z_2} \max_{z_2} K[z_1, z_2]. \qquad (3)$$

В основу разработанного программного комплекса для решения этой задачи положен разработанный в [6] численный алгоритм.

Противоборство (дифференциальная игра) между подвижными управляемыми объектами. Используя (по возможности) систему обозначения и основные положения, изложенные в [6], развивая эти положения, рассмотрим следующую игровую задачу противоборства между подвижными управляемыми объектами.

Игроки 1 и 2, участвующие в игре, располагают L_1 и L_2 подвижными объектами (системами) соответственно, которые в начале игры находятся в точках $\bar{r}^1_{k0}$, $1 \le k \le L_1$ и $\bar{r}^2_{k0}$, $1 \le k \le L_2$ пространства противоборства. В дальнейшем, под понятиями подвижный объект и подвижная система будем понимать одно и то же — противоборствующий объект. Обозначим через t_{kf} время движения (полета) k-го объекта, управляемого q-м игроком ($q = 1, 2$), от точки $\bar{r}^q_{k0}$ до точки $\bar{r}^q_{kf}$.

Очевидно, что число t_{kf} (время движения k-го объекта) зависит от траектории $\bar{r}^q_k = \bar{r}^q_k(t)$, выбираемой в процессе игры q-м игроком для управления k-м подвижным объектом, причем $\bar{r}^q_k(0) = \bar{r}^q_{k0}$ и $\bar{r}^q_k(tf) = \bar{r}^q_{kf}$.

На траектории всех подвижных объектов $\bar{r}^q_k(t)$, $q = 1, 2$, $1 \le k \le L_q$, и законы их движения наложим те же ограничения, что и в [6].

Противоборствующие стороны динамически активно влияют друг на друга при приближении k-го объекта, управляемого q-м игроком, к подвижному объекту противоборства на расстояние дальности активного взаимодействия, используя для этого

соответствующие механизмы воздействия на увеличение интенсивности отказов противоборствующей системы, то есть уменьшая вероятность ее безотказной работы (функциональную надежность), приводящую, в конечном итоге, к отказу системы в целом.

Обозначим через p_{kq} вероятность безотказной работы k-го подвижного объекта, управляемого q-м игроком; $q=1,\ 2;\ 1\le k\le L_q$; λ_{kq} — интенсивность отказов соответствующего k, q-объекта. Тогда, при аппроксимации поведения в процессе игры противоборствующих подвижных объектов неоднородным марковским процессом [7], игра может быть описана следующей системой дифференциальных уравнений Колмогорова:

$$p'_{kq}(t)=-\lambda_{kq}p_{kq}(t),\quad q=1,\ 2 \qquad (4)$$

с начальными условиями $p_{k0}(0)=1$,
где

$$k=\begin{cases}1,\ 2,\ ...,\ L_1 \text{ при } q=1,\\ 1,\ 2,\ ...,\ L_2 \text{ при } q=2,\end{cases} \qquad (5)$$

а интенсивность отказов λ_{kq} определяется из указанных выше условий противоборства подвижных систем следующим образом:

$$\lambda_{k1}=\lambda_k^1(t,\bar{r}_k^{-1})+\sum_{i=1}^{L_2}\frac{b_{i2}\left(\left|\bar{r}_k^{-1}-\bar{r}_i^{-2}\right|\right)}{\left|\bar{r}_k^{-2}-\bar{r}_i^{-1}\right|^{\alpha(i,2)}}, \qquad (6)$$

$$\lambda_{k2}=\lambda_k^2(t,\bar{r}_k^{-2})+\sum_{i=1}^{L_1}\frac{b_{il}\left(\left|\bar{r}_k^{-2}-\bar{r}_i^{-1}\right|\right)}{\left|\bar{r}_k^{-2}-\bar{r}_i^{-1}\right|^{\alpha(i,l)}}, \qquad (7)$$

при этом величина

$$b_{kq}(x)=\begin{cases}0, \text{ если } x>\gamma_{kq};\\ 1, \text{ если } x\le\gamma_{kq}.\end{cases} \qquad (8)$$

В связи с тем, что дифференциальные уравнения в системе уравнений Колмогорова имеют переменные коэффициенты, поскольку интенсивность отказов противоборствующих систем зависит от многих переменных и изменяется в пространстве и времени, то получить аналитическое решение для вычисления безотказной работы p_{kq} каждого k-го подвижного объекта $1\le k\le L_q$, управляемого q-м ($q=1,\ 2$) игроком не представляется возможным.

Поэтому для решения этой системы дифференциальных уравнений следует использовать математический аппарат метода дискретизации, разработанный для решения подобных задач в [5].

Очевидно, что в рассматриваемой задаче противоборства между подвижными объектами, описываемой дифференциальной игрой, множеством стратегий W^q q-го игрока является множество траекторий $\bar{r}_k^q(t)$ соответствующего подвижного объекта, участвующего в противоборстве, то есть

$$W^q=\left\{\bar{r}_k^q(t)\middle|1\le k\le L_q\right\},\ q=1,\ 2. \qquad (9)$$

В качестве функции выигрыша примем

$$K[z_1,z_2]=\sum_{k=1}^{L_1}p_{k1}(t_{kf})-\sum_{k=1}^{L_2}p_{k2}(t_{kf}), \qquad (10)$$

где $z_q\in W^q$, а t_f — заданное время игры.

Тогда решением рассматриваемой задачи, так же как и в предыдущем разделе, является вычисление оптимальных стратегий $\tilde{z}_1$ и $\tilde{z}_2$, для которых

$$K[\tilde{z}_1,\tilde{z}_2]=\min_{z_2}\max_{z_2}K[z_1,z_2]. \qquad (11)$$

В результате дифференциальная игра сводится к матричной и её решение ищется в смешанных стратегиях [7].

Описание программного комплекса для решения двух поставленных задач. Разработанный программный комплекс (далее ПК) для проведения вычислительных экспериментов реализует разработанные авторами работы численные алгоритмы для решения задач оптимального управления противоборствующими подвижными и неподвижными объектами и оптимального управления противоборствующими подвижными управляемыми объектами. ПК разработан в среде «C#», для которой характерны универсальность, широкие возможности решения инженерных задач и удобство работы с интерфейсом.

За основу разработки ПК принята математическая модель и алгоритм решения игровой задачи типа «нападение – защита» для двух игроков, располагающих подвижными (нападающими) и неподвижными (защищающимися) объектами (системами) соответственно, которая подробно описана в [6].

ПК выполняет следующие основные функции:

— ввод исходных параметров игровых задач;

— расчет интенсивности отказов подвижного объекта;

— расчет вероятности безотказной работы противоборствующего подвижного объекта;

— вычисление траектории движения управляемых подвижных объектов, с указанием значения вектора расположения объектов;

— вычисление оптимальной стратегии каждого из игроков, с указанием координат, задающих начальную точку, время полета и значения интенсивности отказов игрока.

Общий алгоритм работы программы представлен на рис. 1.

Работа ПК осуществляется следующим образом. Программа ожидает нажатие кнопки «Рассчитать» от пользователя, после чего запускает алгоритм «рассчитать». Данные, введённые пользователем, считываются из соответствующих элементов и проверяются на соответствие входному формату. Если все данные введены корректно, то программа начинает определение наилучших стратегий поведения для атакующих и защищающихся объектов.

Данный ПК выполняет расчет интенсивности отказов подвижного объекта, вероятности безотказной работы противоборствующего подвижного объекта, вычисление траектории движения управляемых подвижных объектов, с указанием значения вектора расположения объектов, вычисление оптимальной стратегии каждого из игроков, с указанием координат, задающих начальную точку, время полета и значения интенсивности отказов игрока.

Интерфейс ПК имеет следующий вид (рис. 2). В ПК предусмотрено пять окон:

— окно ввода данных первого игрока;

— окно ввода данных второго игрока;

— окно «Пункты защиты второго игрока»;

— «Результаты вычислений»;

— «Игровое поле».

После загрузки программы откроется окно ввода параметров (рис. 2), где необходимо задать основные

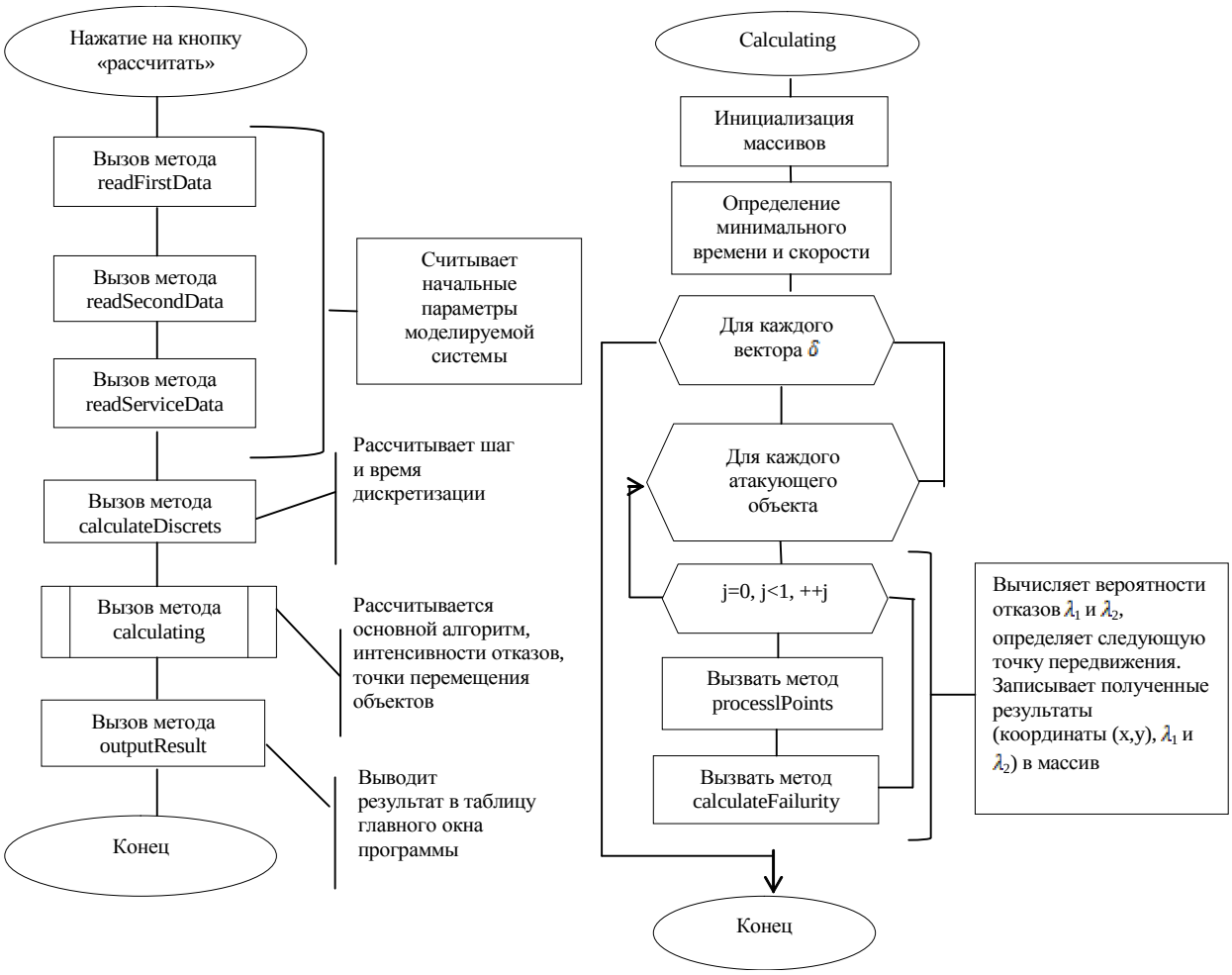


Рис. 1. Общий алгоритм работы программы

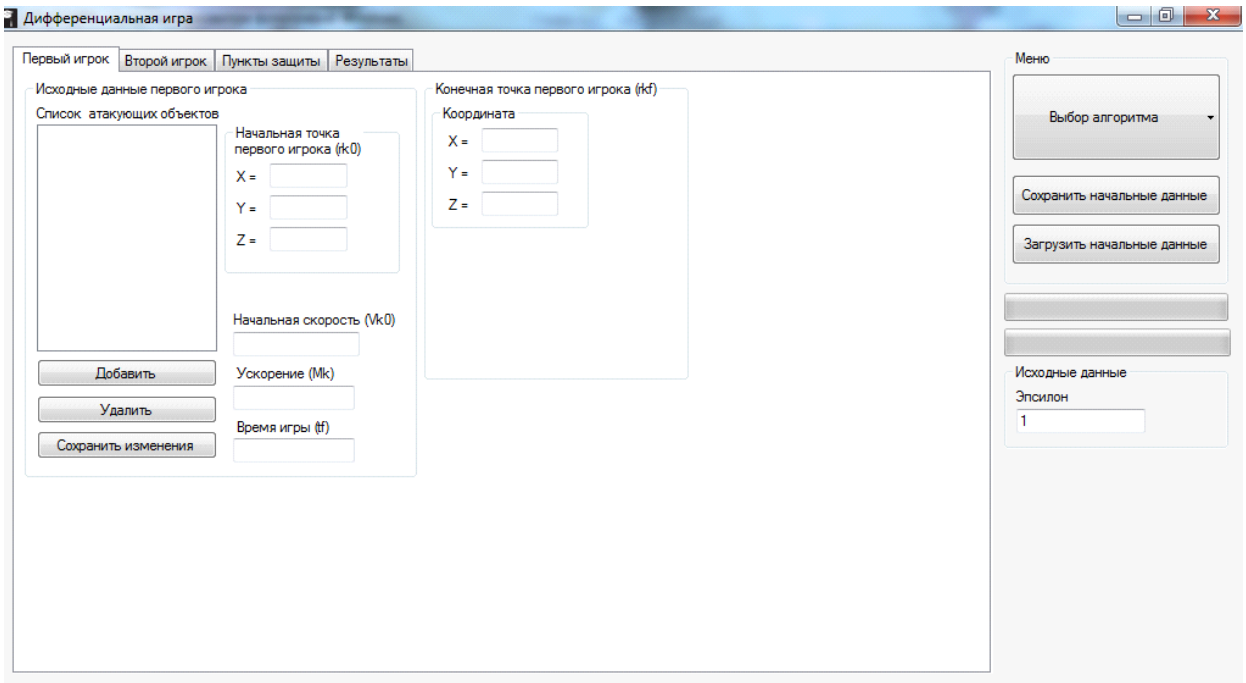


Рис. 2. Интерфейс ПК

параметры игроков, обеспечивающих оптимальное решение:

— координаты атакующего объекта;
— интенсивность отказов;
— начальная скорость;
— начальное ускорение;
— время игры t_f;
— координаты защищаемых объектов;
— количество точек защиты;
— точность измерения ε.

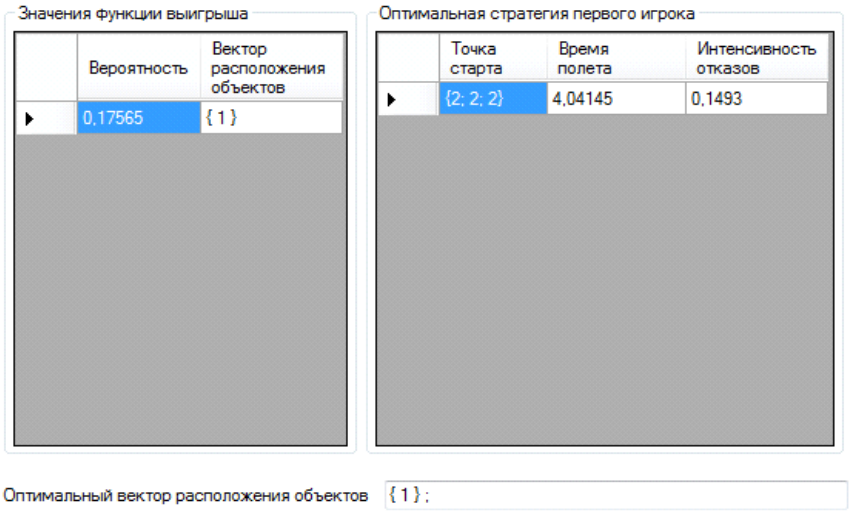


Рис. 3. Результаты расчета ПК

Затем из выплывающего окна кнопки «Выбор алгоритма» нужно выбрать дифференциальную игру, алгоритм которой будет выполнять программа. После нажатия кнопки «Рассчитать» программа переходит в окно расчетов (рис. 3).

На рис. 3. формируется отчет о результатах расчета программы.

Результатом вычислений программы является максимальное значение функции выигрыша K_j, т.е. определение оптимальной пространственно-временной стратегии резервирования подвижного объекта. Указывается значение, вероятности безотказной работы противоборствующего подвижного объекта, координаты вектора расположения объекта.

Затем идут основные вычисления оптимальной стратегии первого игрока:

— номер объекта;

— координаты объекта;

— время полета атакующего объекта;

— интенсивность отказов.

Стоит еще раз отметить, что все вычисления проводятся на каждом j-ом шаге до тех пор, пока не произойдет максимальное приближение подвижного объекта к неподвижному на заданное расстояние, т.е. вычисление максимального значения функции выигрыша.

Для повышения надежности и эффективности проведения исследования, правильной интерпретации результатов, а также чтобы не загромождать окно программы результатами вычислений, выходные данные программы задаются для шага, на котором определена оптимальная стратегия подвижного объекта.

В ходе экспериментов изменять значения параметров можно как с помощью вызова окна ввода параметров, так и непосредственно на панели изменения основных параметров системы главного окна программы.

Заключение. На разработанный программный комплекс для оптимального управления противоборствующими объектами получено свидетельство о государственной регистрации электронного ресурса № 2014617425 [8]. Данный ПК может использоваться как в исследовательских, так и в практических целях. В основу разработанного ПК был заложен модульный принцип построения программ, что обеспечивает возможность дальнейшего расширения его функциональных возможностей.

Библиографический список

1. Потапов, В. И. Постановка двух задач оптимального управления подвижной, структурно-перестраиваемой избыточной системой, управляемой по каналам связи / В. И. Потапов // Динамика систем, механизмов и машин : материалы VII Междунар. науч.-техн. конф., посвящ. 70-летию ОмГТУ. — Омск : ОмГТУ, 2012. — С. 276—278.

2. Красовский, Н. Н. Управление динамической системой / Н. Н. Красовский. — М. : Наука, 1985. — 517 с.

3. Потапов, В. И. Математическая модель и алгоритм оптимального управления подвижным объектом в конфликтной ситуации / В. И. Потапов // Мехатроника, автоматизация, управление. — 2014. — № 7 (160). — С. 16—22.

4. Потапов, В. И. Противоборства (дифференциальная игра) двух нейрокомпьютерных систем / В. И. Потапов, И. В. Потапов // Информационные технологии. — 2005. — № 8. — С. 53—57.

5. Потапов, В. И. Новые задачи оптимизации резервированных систем / В. И. Потапов, С. Г. Братцев. — Иркутск : Изд-во Иркутск. ун-та, 1986. — 112 с.

6. Потапов, В. И. Дифференциальная игра между подвижными и неподвижными объектами / В. И. Потапов // Омский научный вестник. Сер. Приборы, машины и технологии. — 2012. — № 3 (113). — С. 268—271.

7. Оуэн, Н. Г. Теория игр и игровое моделирование. Исследование операций. Методологические основы и математические методы : в 3-х т. / Н. Г. Оуэн. — М. : Мир, 1981. — Т. 1. — С. 513—549.

8. Горн, О. А. Программа для решения задач оптимального управления противоборствующими подвижными объектами / В. И. Потапов, О. А. Горн // Свидетельство о регистрации электронного ресурса № 2014617425 от 22.07.2014 г. — М. : ФИПС, 2014.

ПОТАПОВ Виктор Ильич, доктор технических наук, профессор (Россия), заведующий кафедрой «Информатика и вычислительная техника», заслуженный деятель науки и техники РФ.

ГОРН Ольга Анатольевна, аспирантка, ассистент кафедры «Информатика и вычислительная техника».

Адрес для переписки: Anatole4ka@yandex.ru

Статья поступила в редакцию 08.04.2015 г.

УДК 519.863:687.01

Л. Ф. НЕМИРОВА
С. Б. КАТАЕВА

Омский государственный институт сервиса

ОПТИМИЗАЦИЯ ВЫБОРА МАТЕРИАЛОВ ДЛЯ МОДЕЛЕЙ И КОЛЛЕКЦИИ ОДЕЖДЫ

В статье рассматривается задача оптимального выбора материалов для коллекций одежды с применением моделей и методов дискретной оптимизации. Дается математическая постановка задачи, представляющая собой обобщение известной задачи о покрытии множества. Показаны принципы формирования коллекций одежды с определенным визуальным разнообразием.

Ключевые слова: дизайн, визуальное разнообразие, выбор материалов, коллекция, теория графов, целочисленное линейное программирование.

Введение. Создавая коллекции, предприятие стремится использовать оптимальное количество материалов, ограничивая выбор поставщиками, ценой и др., при этом должно обеспечиваться визуальное разнообразие моделей.

Задача оптимизации выбора материалов сформулирована и рассмотрена в ряде работ, выполненных в Омском государственном институте сервиса [1 – 5]. Применение математических методов и моделей существенно повышает объективность принимаемых решений.

В статье рассматривается выбор материалов дизайнерами и анализ результатов с применением предложенных методов.

Прикладная задача проектирования коллекции одежды формулируется следующим образом:

— имеются эскизы моделей коллекции одежды и образцы материалов;

— из образцов выбирается набор материалов для изготовления коллекции;

— выбор осуществляется группой специалистов;

— задаются определенные условия проектирования коллекции:

— обеспечение визуального разнообразия каждой модели;

— использование фиксированного числа материалов в наборе [1 – 4].

Представим исходные условия задачи следующим образом:

— имеется m моделей одежды, $W=\{w_1, w_2, \ldots w_m\}$;

— имеется n образцов материалов, $V=\{v_1, v_2, \ldots v_n\}$;

— в выборе материалов принимает участие s экспертов;

— для обеспечения визуального разнообразия каждая модель коллекции будет изготовлена из заданного числа материалов b_i, где $b=1, 2, \ldots n$;

— задаётся верхняя граница числа материалов в наборе — k, из которого будет изготавливаться коллекция, где $k \le n$.

Для решения используется теория графов и целочисленное линейное программирование (ЦЛП), в частности обобщенная задача о наименьшем покрытии множества [5, 6].

Рассматривается двудольный граф $G=(\overline{V}, E)$ с множеством вершин V и множеством ребер E. Вершины соответствуют материалам и моделям: $\overline{V}=(V \cup W)$, где $V=\{v_1, \ldots, v_n\}$ вершина v_j отвечает j-му материалу, $j=1, \ldots, n$, а $W=\{w_1, \ldots, w_m\}$, w_i соответствует i-ой модели одежды, $i=1, \ldots, m$. Ребро Е отражает выбор: если j-ый материал выбран для изготовления i-ой модели, то в Е имеется ребро (v_j, w_i), $j=1, \ldots, n$, $i=1, \ldots, m$. Двудольному графу G соответствует матрица смежности A.

Допустимое b-покрытие для двудольного графа определяется следующим образом. Пусть V' — подмножество вершин V ($V' \subseteq V$) и E' — совокупность всех инцидентных с V' ребер. Множество V' называется допустимым b-покрытием, если любая вершина w_i является концом не менее b_i ребер из E'.

Число материалов для каждой модели в коллекции задается целочисленным вектором $b=(b_1, b_2, \ldots, b_i)^v$, где b_i заданное число материалов, выбранных для i ой модели; $i=1, \ldots, m$; $b_i < n$.

Задача заключается в нахождении допустимого b-покрытия минимальной или заданной мощности.

Для формулировки соответствующей задачи ЦЛП вводятся следующие обозначения.

Пусть a_{ij} — компоненты матрицы смежности A:

$$a_{ij}=\begin{cases}1, \text{ если } i\text{-й материал выбран для } j\text{-го изделия,}\\ 0, \text{ в противном случае,}\end{cases}$$

где $i=1, \ldots, m$, $j=1, \ldots, n$.

Для материала вводится переменная его выбора (включения в набор)

$$x_{ij}=\begin{cases}1, \text{ если } i\text{-й материал включён в набор,}\\ 0, \text{ в противном случае,}\end{cases}$$

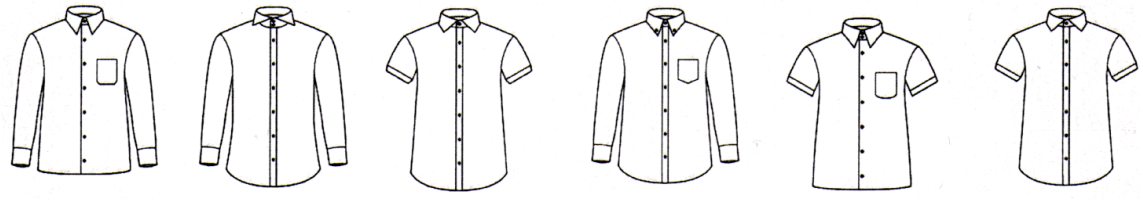
где $j=1, \ldots, n$.

Модель ЦЛП имеет вид:

$$\sum_{j=1}^{n} x_j \to \min \ , \qquad (1)$$

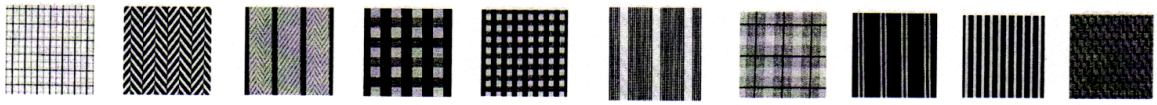
при условиях

$$\sum_{i=1}^{n} a_{ij} x_j \ge b_i \ , \quad i=1, \ldots, m, \qquad (2)$$



№ 1 № 2 № 3 № 4 № 5 № 6

Рис. 1. Эскизы моделей мужской сорочки



№ 1 № 2 № 3 № 4 № 5 № 6 № 7 № 8 № 9 № 10

Рис. 2 Образцы материалов

Таблица 1

Матрица относительной пригодности материалов

		Материалы									
		1	2	3	4	5	6	7	8	9	10
Модели	1	0,22	0,67	0,00	0,78	0,22	0,45	0,56	0,22	0,89	1,00
	2	0,67	0,56	0,67	0,44	0,56	0,44	0,44	0,33	0,67	0,22
	3	0,44	0,67	0,33	0,56	0,56	0,56	0,67	0,44	0,44	0,33
	4	0,67	0,33	0,44	0,56	0,44	0,33	0,78	0,33	0,56	0,56
	5	0,44	0,44	0,56	0,56	0,44	0,56	0,44	0,33	0,56	0,67
	6	0,67	0,67	0,67	0,56	0,22	0,56	0,33	0,67	0,33	0,33

$$x_j \in \{0,1\},\ j=1,\ \ldots,\ n. \qquad (3)$$

При разработке коллекций на предприятии количество материалов и моделей невелико, в этой ситуации решаемая задача имеет малую размерность. Она решается перебором булевых векторов, который ведется по слоям, соответствующим значениям целевой функции. Для каждого вектора проверяется, удовлетворяет ли он системе (2), если да, то вычисляется значение целевой функции (1).

Если задаётся фиксированное число материалов в наборе k, необходимо найти решение системы ограничений

$$\sum_{j=1}^{n} x_j \le k\ , \qquad (4)$$

$$\sum_{i=1}^{n} a_{ij} x_j \ge b_i\ ,\ i=1,\ \ldots,\ m, \qquad (5)$$

$$x_j \in \{0,1\},\ j=1,\ \ldots,\ n. \qquad (6)$$

Для реализации предложенного метода разработано пользовательское приложение в среде Delphi [3].

Решение задачи проектирования коллекции. Задача выбора материалов рассмотрена на примере мужских сорочек. Коллекция включает 6 моделей, отличающихся назначением, силуэтами, длиной рукава, формой воротника, планки и кармана (рис. 1). Выбор проводился из десяти образцов сорочечных тканей, изображения которых представлены на рис. 2.

В эксперименте участвовали 6 специалистов. При выборе применен метод парных сравнений [7]: дизайнер сравнивал первый материал с остальными, затем — второй, третий и т. д., занося результаты в соответствующую таблицу.

Для оценки результатов коллективного выбора материалов предложена характеристика «пригодность» и установлены её критерии [3–4]. Величина показателя пригодности является мерой приближения каждого оцениваемого материала к некоторому идеальному, полностью соответствующему данной модели.

Пригодность характеризуется относительной частотой предпочтений при выборе P_i; где $P_i \in [0,1]$.

$$P_i = \frac{\sum_{j=1}^{n} d_{ij}}{(n-1)\times s}\ , \qquad (7)$$

где d_{ij} — оценка предпочтения i-го материала j-м экспертом; n — число материалов; $(n-1)$ — число сопоставлений; s — число экспертов; $i,\ j=1,\ 2,\ \ldots,\ n$.

Значения показателя пригодности находятся в интервале от 0 до 1. При этом j-ый материал выбран для модели, если показатель относительной пригодности $\Delta P_j \le R$. В качестве граничных точек критерия R установлены значения: 0,37; 0,63; 0,80. При значении от 0,37 до 0,63 — пригодность удовлетворительная; 0,64 и 0,80 соответствуют нижним значениям хорошей и отличной пригодности [3].

По итогам выбора материалов экспертами по формуле (7) определена пригодность каждого из десяти материалов (табл. 1). Результаты соответствия моделей мужских сорочек и образцов материалов при критерии пригодности $R \ge 0,63$ отображены в табл. 2.

Полученные результаты представлены в виде двудольного графа (рис 3), и соответствующей ему матрицы смежности (табл. 3). Фрагмент графа на примере мужской сорочки № 2 показан на рис. 4.

Таблица 2

Выбор материалов для моделей сорочки при R>0,63

Модели	Материалы										

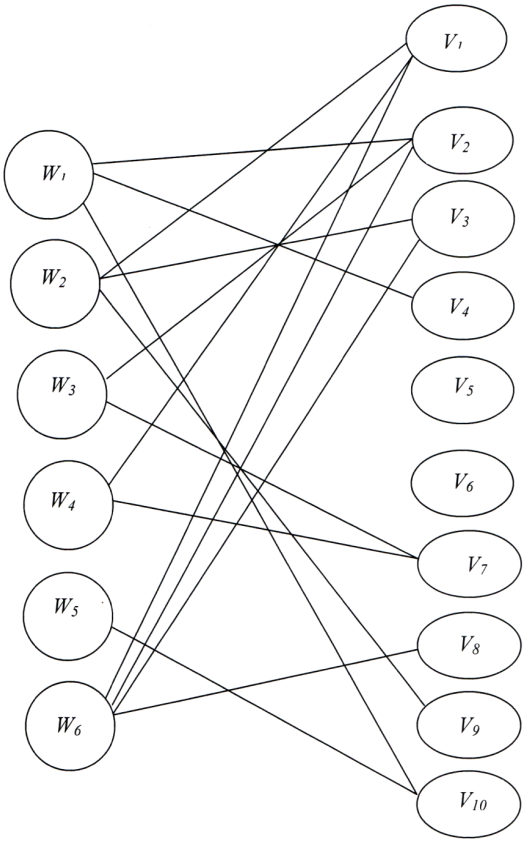


Рис. 3. Двудольный граф

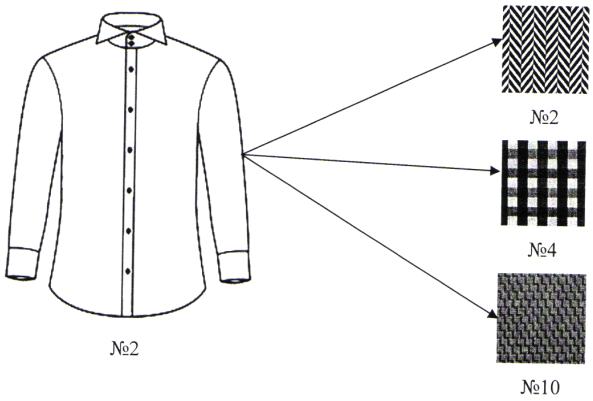


Рис. 4. Двудольный граф, иллюстрирующий выбор материала

Рассмотрим выбор материалов для следующих условий проектирования коллекции.

Условие 1: получить набор материалов для коллекции с заданным визуальным разнообразием.

В коллекции для каждой модели предполагается использовать по одному материалу, это может быть один материал для всех моделей либо различные материалы. Соответствующая запись вектора покрытия: $b = (1, 1, 1, 1, 1, 1)$.

Таких наборов материалов два. Минимальное число материалов в наборе равно трем. Первый набор включает образцы 3, 7, 10; второй набор — образцы 1, 2, 10. При этом обеспечивается внешнее различие моделей, а при окончательном выборе можно учитывать цену материалов, поставщиков и др.

Таблица 3

Матрица смежности материалов

a_{ij}		Материалы										
		1	2	3	4	5	6	7	8	9	10	$a_{ij}\ x_j$
Модели	1	0	**1**	0	**1**	0	0	0	0	0	**1**	3
	2	**1**	0	**1**	0	0	0	0	0	**1**	0	3
	3	0	**1**	0	0	0	0	**1**	0	0	0	2
	4	**1**	0	0	0	0	0	**1**	0	0	0	2
	5	0	0	0	0	0	0	0	0	0	**1**	1
	6	**1**	**1**	**1**	0	0	0	0	**1**	0	0	4
	Σx_j	3	3	2	1	0	0	2	1	1	2	

Для каждой модели предполагается использовать по два материала. Вектор покрытия задается следующим образом: $b=(2, 2, 2, 2, 2, 2)$.

Из полученных результатов (табл. 2) следует, что при таком условии решение не может быть найдено, поскольку для пятой модели выбран всего один материал. То есть возможный вектор покрытия $b=(2, 2, 2, 2, 1, 2)$.

Условие 2: для коллекции необходимо использовать фиксированное число материалов. Задается число материалов в наборе $k=4$.

При условии $b=(2, 2, 2, 2, 1, 2)$ оптимальным является набор, включающий материалы 1, 2, 9, 10.

Если при этом же условии для коллекции необходимо использовать не более шести материалов, $k=6$, оптимальным является набор, включающий материалы 3, 4, 7, 8, 9, 10.

Заключение. Рассмотренный подход и его реализация позволяют проектировать коллекции одежды в соответствии с установленными требованиями, обеспечить объективность выбора и экономическую эффективность производства за счет применения ограниченного набора материалов.

Библиографический список

1. Немирова, Л. Ф. К вопросу о конфекционировании материалов для одежды / Л. Ф. Немирова // Швейная промышленность. – 1997. – № 6. – С. 15–16.

2. Катаева, С. Б. Автоматизация проектирования трикотажных изделий с учётом структуры и свойств нитей и полотен : автореф. дис. ... канд. техн. наук / С. Б. Катаева. – Омск : ОГИС, 2006. – 17 с.

3. Мирончик, Е. В. Автоматизация подбора материалов для одежды на основе аналитических методов : автореф. дис. ... канд. техн. наук / Е. В. Мирончик. – Омск : ОГИС, 2010. – 19 с.

4. Немирова, Л. Ф. Решение задачи выбора материалов для моделей одежды / Л. Ф. Немирова, Е. В. Мирончик // Известия высших учебных заведений. Технология лёгкой промышленности. – 2012. – Т. 15, № 1. – С. 41–45.

5. Колоколов, А. А. Решение задачи подбора материалов на основе методов дискретной оптимизации / А. А. Колоколов, Л. Ф. Немирова, С. Б. Катаева // Динамика систем механизмов и машин : материалы VI Междунар. науч. конф. – Омск : ОмГТУ, 2007. – Кн. 3 – С. 46–48.

6. Еремеев, А. В. Задача о покрытии множества: сложность, алгоритмы, экспериментальные исследования / А. В. Еремеев, Л. А. Заозерская, А. А. Колоколов // Дискретный анализ и исследование операций. Сер. 2. – 2000. – Т. 7, № 2. – С. 22–46.

7. Гвишиани, Д. М. Многокритериальные задачи принятия решений / Д. М. Гвишиани, С. В. Емельянова. – М. : Машиностроение, 1978. – 192 с.

НЕМИРОВА Любовь Фёдоровна, кандидат технических наук, доцент (Россия), доцент кафедры конструирования и технологий лёгкой промышленности.
КАТАЕВА Светлана Борисовна, кандидат технических наук, доцент кафедры дизайна костюма.
Адрес для переписки: kataevasvetlana@mail.ru

Статья поступила в редакцию 26.03.2015 г.

Книжная полка

Лафоре, Р. Структуры и алгоритмы JAVA / Роберт Лафоре ; пер. с англ. Е. Матвеева. – 2-е изд. – СПб. [и др.] : Питер, 2014. – 701 с. – ISBN 978–5–496–00740–5.

Издание одной из самых авторитетных книг по программированию посвящено использованию структур данных и алгоритмов. Алгоритмы — это основа программирования, определяющая, каким образом разрабатываемое программное обеспечение будет использовать структуры данных. На четких и простых программных примерах автор объясняет эту сложную тему, предлагая читателям написать собственные программы и на практике освоить полученные знания. Рассматриваемые примеры написаны на языке Java, хотя для усвоения материала читателю не обязательно хорошо знать его — достаточно владеть любым языком программирования, например, C++. Первая часть книги представляет собой введение в алгоритмизацию и структуры данных, а также содержит изложение основ объектно-ориентированного программирования. Следующие части посвящены различным алгоритмам и структурам данных, рассматриваемым от простого к сложному: сортировка, абстрактные типы данных, связанные списки, рекурсия, древовидные структуры данных, хеширование, пирамиды, графы. Приводятся рекомендации по использованию алгоритмов и выбору той или иной структуры данных в зависимости от поставленной задачи.

УДК 004.7385.5

Е. Б. ЮДИН
В. Н. ЗАДОРОЖНЫЙ

Омский государственный технический университет

РАСЧЕТ ЧИСЛА СЕТЕВЫХ МОТИВОВ МЕТОДОМ СЛУЧАЙНОЙ ВЫБОРКИ КАРКАСОВ

Разработка эффективных алгоритмов анализа сетевых мотивов является таким направлением в Network Science, которое имеет большое значение при исследовании сетей связи, социальных, биологических и других сетей. Формально обнаружение мотивов и расчет их числа представляет собой обнаружение и подсчет типовых изоморфных подграфов в больших графах. В статье для ускорения этой процедуры разрабатывается метод случайной выборки каркасов (МВК), основанный на методе Монте-Карло. Приводятся примеры подсчета в неориентированном графе типовых подграфов на трех и на четырех вершинах. Предлагаемый подход может также быть расширен и для анализа больших ориентированных графов.

Ключевые слова: сетевые мотивы, подсчет подграфов, системный анализ.

Работа выполнена при поддержке гранта РФФИ 14-01-31551-мол_а.

Введение. Последние десятилетия характеризуются появлением баз данных о существующих сетевых системах, а также постоянно растущей производительностью компьютеров и быстрым развитием мощных программных инструментов анализа больших сетей. Это позволяет изучать влияние структурных характеристик реальных сетей, содержащих сотни тысяч узлов, на качество функционирования этих сетей. Такие исследования охватывают сети передачи данных, социальные, биологические и другие сети [1 – 3].

Одной из задач анализа структурных характеристик больших сетей является задача распознавания сетевых мотивов и их подсчета. Сетевые мотивы представляют собой типовые связные подграфы на заданном числе вершин, причем, как правило, имеются в виду подграфы, которые встречаются в исследуемой реальной сети чаще, чем в рандомизированном графе с тем же распределением степени связности [4]. Частота встречаемости различных сетевых мотивов — это важная многомерная числовая характеристика структуры большой сети [5, 6].

Задача обнаружения и подсчета сетевых мотивов представляет собой задачу высокой вычислительной стоимости. Эта задача подразумевает подсчет подграфов в исходном графе и в его рандомизированной версии. В последние годы в числе программных инструментов, разработанных для анализа больших сетей, появилось много алгоритмов обнаружения и подсчета мотивов [7 – 11].

Среди разработанных алгоритмов подсчета мотивов можно выделить MFINDER [7], который был разработан в 2003 году, а также FANMODE (2006) [8] и KAVOSH (2009) [9], которые по производительности превзошли своих предшественников. Такие программы как igraph (R-пакет) и NetMODE используют в качестве базиса именно эти алгоритмы. Алгоритм MFINDER используется в качестве базиса в проекте mDraw.

Подсчет в пакетах mDraw и igraph мотивов на трех и четырех вершинах (3- и 4-мотивов), содержащихся в сети автономных систем Интернет [12] (22963 вершин и 48436 ребер), характеризуется высокой вычислительной стоимостью. Пакет mDraw на современном персональном компьютере затрачивает на поиск 3-мотивов 11,67 минут, 4-мотивов — более двух суток. Пакет R выполняет поиск 3-мотивов за 49 секунд, 4-мотивов — за 2 часа 13 минут.

В ряде случаев алгоритмы, используемые в популярных пакетах, могут быть улучшены за счет оптимизации проверки изоморфизма подграфов [10 – 11]. Сложность получаемых алгоритмов оценивается как $O(|E|)$ и $O(|E|^2)$ для 3- и 4-мотивов соответственно, где $|E|$ — число ребер в графе. В данной работе для ускорения подсчета мотивов разрабатывается *метод случайной выборки каркасов* (МВК), основанный на применении метода Монте-Карло.

1. Постановка задачи. Рассмотрим задачу определения для заданного графа G числа 3- и 4-мотивов, представленных на рис. 1.

2. Решение. Для ускорения процедуры подсчета мотивов будем использовать метод Монте-Карло — численный метод, основанный на получении большого числа N реализаций случайного процесса, который формируется таким образом, чтобы его вероятностные характеристики совпадали с искомыми величинами решаемой задачи. Для расчета числа мотивов типа Motif 3_2 нашим методом многократно реализуется случайный (равновероятный) выбор одной из вилок (путей длины 2) графа G и определяется вероятность P_{3_2} того, что на вершинах выбранной вилки лежит подграф Motif 3_2 (треугольник). После этого число вилок, содержащих Motif 3_2, определяется произведением $P_{3\_2}{\cdot}N_v$, где N_v — число вилок в графе G. И, поскольку любой один и тот же треугольник содержат три вилки, искомое число треугольников N_Δ определяется формулой:

$$N_\Delta = P_{3\_2} \cdot N_v / 3. \qquad (1)$$

Для реализации описанного подхода требуется a) найти используемое в (1) число N_v всех вилок в графе G и b) обеспечить случайный равновероятный выбор вилок. Оба требования выполняются за

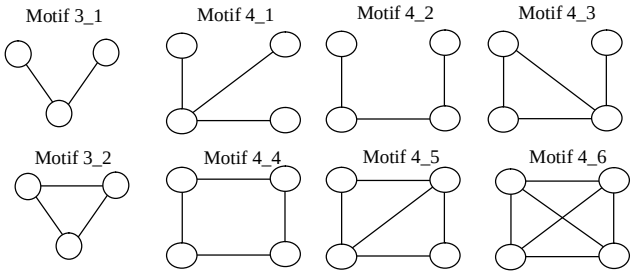


Рис. 1. Возможные 3- и 4-мотивы

Input: Graph (V, E), N
Output: *motif*3_1, *motif*3_2
1. $A_1 < \varnothing, A_2 < \varnothing, \ldots$; *count*_1 < 0, *count* _2< 0, *sum* < 0
2. **foreach** $v \in$ V **do**
   $k <$ |Adj(v)|, *sum* < *sum* + $k\times(k-1)/2$, Add v to A_k **end**
3. **foreach** A_k **do** $P_k <$ $|A_k|\times k\times(k-1)/2$ /*sum* **end**
4. **for** $i = 1, N$ **do**
   Generate $r\sim\{P_k\}$
   $v <$ get from A_r random
   $v1, v2 <$ get from Adj(v) random ($v2 \neq v1$)
   if $v1 \in$ adj ($v2$) **then** *count* _2 < *count* _2 + 1
   else *count* _1 < *count* _1 + 1
   end
5. *motif*3_1< *count*_1/$N\times$*sum*
   *motif*3_2< *count* 2 / $N\times$*sum* /3
return *motif*3_1, *motif*3_2

Рис. 2. Алгоритм подсчета 3-мотивов

Таблица 1

Расчеты числа подграфов типа MOTIF 3_2

Исследуемые сети	Расчет числа подграфов		
	Полный перебор	МВК	
		N=1 000	N=100 000
Internet	140 538	$1{,}7\cdot10^5$	$1{,}400\cdot10^5$
Gnutella	6 069	$6{,}4\cdot10^3$	$5{,}9\cdot10^3$
Email-Enron	2 181 111	$2{,}14\cdot10^6$	$2{,}18\cdot10^6$
PGP network	164 362	$1{,}69\cdot10^5$	$1{,}643\cdot10^5$

Таблица 2

Расчеты вероятности P_{3_2} с относительной погрешностью 1 %

Исследуемые сети	МВК	
	Число опытов N	Оценка вероятности P_{3_2}
Internet	2 000	0,012
Gnutella	5 200	0,0040
Email-Enron	1 500	0,088
PGP network	1 300	0,38

счет однократного просмотра всех вершин графа и распределения их по подмножествам (слоям) A_k, содержащим вершины с одинаковой степенью связности k ($k = 1, 2, \ldots$). В результате такого расслоения число вилок в графе вычисляется по формуле

$$N_v = \sum_k |A_k| \cdot \frac{k(k-1)}{2}, \qquad \textbf{(2)}$$

где $|A_k|$ — число вершин в слое A_k. Формула (2) учитывает, что каждая вершина слоя A_k однозначно идентифицирует $k(k-1)/2$ вилок, серединой которых она является.

Равновероятный выбор вилок осуществляется следующей последовательностью выборов:

1) случайно выбирается слой вершин; при этом вероятность P_k выбора слоя A_k пропорциональна числу вилок, серединами которых являются вершины этого слоя:

$$P_k = |A_k| \cdot \frac{k(k-1)}{2} \cdot \frac{1}{N_v}; \qquad \textbf{(3)}$$

2) случайно равновероятно, с вероятностью $|A_k|^{-1}$, выбирается вершина этого слоя;

3) случайно равновероятно выбирается одна из набора вилок, идентифицируемого этой вершиной

Таблица 3

Время расчета 3-мотивов разными методами

Исследуемые сети	Время расчета 3-мотивов, с	
	Полный перебор	МВК, $\nu=0{,}01$
Internet	26,3	1,3
Gnutella	1,9	3,7
Email-Enron	135,3	2,1
PGP network	0,9	0,1

(выбор вилки осуществляется случайным выбором двух инцидентных вершине ребер).

Три шага выбора, ведущие к любой фиксированной вилке графа, имеют вероятности, произведение которых равно $1/N_v$.

Алгоритм расчета числа 3-мотивов, реализующий этот метод, представлен на рис. 2. Через $\mathrm{Adj}(v_i)$ обозначено множество вершин-соседей вершины v_i.

В табл. 1 и 2 приводятся результаты расчета мотивов, полученные описанным методом. Результаты тестирования показывают, что при числе случайно выбранных вилок $N=1\,000$ предложенный метод, обеспечивая значительный выигрыш в скорости расчетов, позволяет оценивать число мотивов с точностью до одной-трех значащих цифр. При проведении 100 тыс. опытов погрешность оценок уменьшается на порядок, а выигрыш в скорости по-прежнему остается существенным. Рассматривались следующие сети: 1) сеть автономных систем Интернет [12] (22 963 вершин, 48 436 ребер); 2) сеть пользователей p2p-сети Gnutella [13] (62586 вершин, 147 892 ребер); 3) сеть адресов электронной почты [13] (36692 вершин, 183 831 ребер); сеть пользователей программы PGP [14] (10 680 вершин, 24 340 ребер).

В качестве критерия точности в табл. 2 используется надежное достижение условия $\nu \le 0{,}01$, где ν — эмпирический коэффициент вариации оценки вероятности P_{3_2}. Из таблицы видно, что для достижения приемлемой точности обычно достаточно 25 000 опытов.

В табл. 3 сравнивается время решения задачи предложенным методом и методом полного перебора.

Алгоритм PROC1 подсчета 4-мотивов типа Motif 4_1 (см. рис. 1), представленный на рис. 3, аналогичен алгоритму подсчета 3-мотивов (рис. 2). Вероятности P_k выбора слоев A_k пропорциональны числу различных «трилистников» (троек ребер), исходящих из вершин слоев. Через subgraph{$v1$, $v2$, $v3$, $v4$} обозначен подграф, лежащий на вершинах $v1$, $v2$, $v3$, $v4$.

Для расчета числа 4-мотивов типа Motif 4_2, ..., Motif 4_6 (рис. 4), выполняется расслоение множества ребер на слои B_s ($s=0,\ 1,\ \ldots$), состоящие из ребер, которые идентифицируют набор s проходящих через них путей длины 3. Всяким ребром однозначно идентифицируется набор (возможно, пустой) всех таких путей длины 3 (включая замкнутые в треугольник), в середине которых лежит это ребро. Число s путей, в середине которых лежит ребро ($v1$, $v2$), равно произведению уменьшенных на единицу степеней вершин $v1$, $v2$:

$$s=(|\mathrm{adj}(v1(e))|-1)\times(|\mathrm{adj}(v1(e))|-1). \qquad \textbf{(4)}$$

Алгоритм PROC2, представленный на рис. 4, обеспечивает равновероятный выбор любого пути из трех

Input: Graph (V, E), *N*
Output: *motif*4_1
1. $A_1 <\ \varnothing$, $A_2 <\ \varnothing$,…
   *count*_1 < 0, *sum* < 0
2. **foreach** $v \in$ V **do**
   $k <$ |Adj(v)|
   sum < *sum* + $k\times(k-1)\times(k-2)/6$
   Add v to A_k
   end
3. **foreach** A_k **do** $P_k <\ |A_k| \times k \times(k-1) \times(k-2)\ /6\ /sum$ **end**
4. **for** $i = 1, N$ **do**
   Generate $r \sim \{P_k\}$
   $v <$ get from A_r random
   $v1,v2\ v3<$ get from Adj(v) random ($v2 \ne v1 \ne v3 \ne v2$)
   if subgraph{$v1,v2,v3,v4$} is motif4_1
   then *count* _1 < *count* _1 + 1
   end
5. *motif4*_1< *count*_1/$N\times$*sum*
return *motif*4_1

Рис. 3. Алгоритм PROC1 подсчета 4-мотивов типа Motif 4_1

Input: Graph (V, E), *N*
Output: *motif*4_2, *motif*4_3, *motif*4_4, *motif4*_5, *motif4*_6
1. $B_1 <\ \varnothing$, $B_2 <\ \varnothing$,…
   *count*_2 < 0, *count*_3 < 0, *count*_4 < 0,
   *count*_5 < 0, *count*_6 < 0, *sum* < 0
2. **foreach** $e \in$ E **do**
   $s = (|\mathrm{adj}(v1(e))| - 1) \times (|\mathrm{adj}(v1(e))| - 1)$
   sum < *s* + *sum*
   Add e to B_s
   end
3. **foreach** B_s **do**
   $P_s <\ |B_s| \times s$ / *sum*
   end
4. **for** $i = 1, N$
   Generate $r \sim \{P_s\}$
   $e <$ get from B_s random
   $v3<$ get from Adj ($v1(e)$) random, $v3 \ne v2$
   $v4<$ get from Adj ($v2$(e)), random $v4 \ne v1$
   if $v3 = v4$ **then** $i = i + 1$, **goto** 4 **end**
   GG< subgraph{$v1,v2,v3,v4$}
   if GG is motif6 **then** *count*_6 < *count*_6 + 1
   else if GG is motif5 **then** *count*_5 < *count*_5 + 1
   else if GG is motif4 **then** *count*_4 < *count*_4 + 1
   else if GG is motif3 **then** *count* _3 < *count*_3 + 1
   else *count*_2 < *count*_2 + 1
   end
5. motif4_2 < *count*_2 /$N \times$ *sum* / 1 ,
   motif4_3 < *count*_3 /$N \times$ *sum* / 2,
   motif4_4 < *count*_4 /$N \times$ *sum* / 4,
   motif4_5 < *count*_5 /$N \times$ *sum* / 6
   motif4_6 < *count*_5 /$N \times$ *sum* / 12
return motif4_2, motif4_3, motif4_4, motif4_5, motif4_6

Рис. 4. Алгоритм подсчета 4-мотивов типа Motif 4_2, ..., Motif 4_6

Таблица 4

Результаты расчета числа 4-мотивов в сети Интернет [12]

Мотивы	Метод расчета		
	igraph	MBK, $N=10\ 000$	MBK, $N=10\ 000\ 000$
Motif 4_1	596 096 955	$5{,}95\cdot10^8$	$5{,}96099\cdot10^8$
Motif 4_2	246 344 022	$2{,}47\cdot10^8$	$2{,}4629\cdot10^8$
Motif 4_3	46 609 744	$4{,}59\cdot10^7$	$4{,}663\cdot10^7$
Motif 4_4	395 305	$3{,}1\cdot10^5$	$3{,}92\cdot10^5$
Motif 4_5	2 350 151	$2\ {,}4\cdot10^6$	$2{,}353\cdot10^6$
Motif 4_6	114 716	$1{,}3\cdot10^5$	$1{,}15\cdot10^5$

ребер за счет последовательного выбора слоя ребер B_s, ребра из этого слоя и пути длины три из набора путей, идентифицируемого этим ребром.

В пункте 5 алгоритма PROC2 число мотивов, «подсчитанное» путями длины 3, делится на коэффициент, равный числу вхождений разных путей длины 3 в соответствующий мотив (см. рис. 1). Этим компенсируется соответствующая кратность «подсчетов» каждого мотива.

В табл. 4 приводится сравнение результатов подсчета мотивов с помощью MBK и с помощью метода FANMODE [8], реализованного в пакете igraph.

Алгоритмы, использующие MBK, запрограммированы на языке Java с использованием библиотеки JUNG [15]. Граф $G=(V, E)$ хранится в виде списка смежных вершин. Сложность предложенных алгоритмов может быть оценена как $O(|V|)$ при расчете числа 3-мотивов и как $O(|E|)$ при расчете числа 4-мотивов. Получаемые оценки — несмещенные, их точность контролируется и может регулироваться числом выполняемых опытов. Метод можно использовать для быстрого и достаточно точного подсчета мотивов в графах, размеры которых не позволяют применять точные методы. Этот метод разработан для применения к неориентированным графам, но его можно адаптировать и для подсчета мотивов в ориентированных графах.

Заключение. В больших графах перебор всех подграфов является вычислительно сложной задачей и по причине их большого размера не всегда может быть выполнен точными методами упорядоченного перебора. В данной статье предложен метод случайной выборки каркасов и соответствующие алгоритмы для ускоренного подсчета числа мотивов, основанные на применении метода Монте-Карло.

Одним из достоинств разработанных алгоритмов является то, что в отличие от других статистических методов (например, от изложенного в [7] метода случайного выбора ребра), эти алгоритмы дают несмещенные оценки числа мотивов и тем самым позволяют корректно выполнять контроль точности оценок в процессе выполнения программы.

Частоту встречаемости определенных конфигураций узлов и связей (мотивов) в реальных сверхбольших сетях необходимо учитывать для построения их адекватных графовых моделей [16, 17].

Библиографический список

1. Pastor-Satorras R., Vespignani A., Evolution and Structure of the Internet: A Statistical Physics Approach Cambridge University Press, Cambridge. — 2004. — Pp. 284.

2. Watts D.J., Strogatz S.H., Collective dynamics of 'small-world' networks // Nature. — 1998. — V. 393. — P. 440.

3. Jeong H., Tombor B., Albert R., Oltvai Z.N., Barabasi A.-L., The large-scale organization of metabolic networks // Nature. — 2000. — V. 407. — P. 651.

4. Milo R., Shen-Orr S., Itzkovitz S., Kashtan N., Chklovskii D., Alon U., Network motifs: simple building blocks of complex networks // Science. — Oct 2002. — V. 298 (5594). — P. 824—827.

5. Kalir S., McClure J., Pabbaraju K., Southward C., Ronen M., Leibler S., Surette M. G., Alon U., Ordering genes in a flagella pathway by analysis of expression kinetics from living bacteria // Science. — Jun 2001. — V. 292(5524). — P. 2080—2083.

6. Mangan S., Zaslaver A., Alon U., The coherent feedforward loop serves as a sign-sensitive delay element in transcription networks // J. Mol. Biol. — Nov 2003. — V. 334(2). — P. 197—204.

7. Kashtan N., Itzkovitz S., Milo R., Alon U., Efficient sampling algorithm for estimating subgraph concentrations and detecting network motifs // Bioinformatics. — Jul. 2004. — V. 20. — № 11. — P. 1746—1758.

8. Wernicke S., Rasche F., Fanmod: a tool for fast network motif detection // Bioinformatics. — 2006. — V. 22. — №. 9. — P. 1152—1153.

9. Kashani Z., Ahrabian H., Elahi E., Nowzari-Dalini A., Ansari E., Asadi S., Mohammadi S., Schreiber F., Masoudi-Nejad A., Kavosh: A new algorithm for finding network motifs // BMC bioinformatics. — 2009. — V. 10. — № 1. — P. 318.

10. Marcus D., Shavitt Y., Efficient counting of network motifs // Proceedings of the 2010 IEEE 30th International Conference on Distributed Computing Systems Workshops, ser. ICDCSW '10. Washington, DC, USA: IEEE Computer Society. — 2010. — P. 92—98.

11. Luis A. Meira A., Vinicius R. Máximo, Álvaro L. Fazenda, Arlindo Flávio da Conceiçãо: acc-Motif: Accelerated Network Motif Detection // IEEE / ACM Trans. Comput. Biology Bioinform. — 2014. — V. 11 (5). — P. 853—862.

12. Newman M., Network data [Электронный ресурс]. — Режим доступа : http://www-personal.umich.edu/~mejn/netdata/ (дата обращения: 15.03.2015).

13. Lescovec Yu., Stanford Large Network Dataset Collection [Электронный ресурс]. — Режим доступа : http://snap.stanford.edu/data/index.html (дата обращения: 15.03.2015).

14. Arenas A., Alex Arenas Website, Network data sets [Электронный ресурс]. — Режим доступа : http://deim.urv.cat/alexandre.arenas/data/welcome.htm (дата обращения: 15.03.2015).

15. JUNG — Java Universal Network / Graph Framework. — [Электронный ресурс]. — Режим доступа : http://jung.sourceforge.net (дата обращения: 15.03.2015).

16. Задорожный, В. Н. Статистически однородные случайные графы: определение, генерация, применение / В. Н. Задорожный, Е. Б. Юдин // Омский научный вестник. Сер. Приборы, машины и технологии. — 2009. — № 3 (83). — С. 7—13.

17. Задорожный, В. Н. Точная теория графа Барабаши—Альберт / В. Н. Задорожный, Е. Б. Юдин // Омский научный

вестник. Сер. Приборы, машины и технологии. — 2009. — № 3 (83). — С. 13—19.

ЮДИН Евгений Борисович, кандидат технических наук, доцент кафедры «Автоматизированные системы обработки информации и управления».
Адрес для переписки: udinev@asoiu.com

ЗАДОРОЖНЫЙ Владимир Николаевич, доктор технических наук, доцент (Россия), профессор кафедры «Автоматизированные системы обработки информации и управления».
Адрес для переписки: zwn@yandex.ru

Статья поступила в редакцию 26.03.2015 г.

УДК 004.083

А. Н. ГРОМОВ
А. П. ТИУНОВ
М. С. ФОМЕНКО
В. Г. ШАХОВ

Омский государственный университет путей сообщения

МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ МНОГОМЕРНЫХ МАТРИЦ

Авторами предложен алгоритм анализа и моделирования информационной безопасности на основе ранее предложенных игровых моделей. Рассмотрены варианты описания безопасности, включая динамическую составляющую, а также варианты количественного оценивания.

Ключевые слова: информационная безопасность, игровая матрица, весовая функция, маршрут, траектория оптимального маршрута.

В практическом анализе информационной безопасности (ИБ) желательно иметь их количественные оценки. Существуют несколько способов количественного описания ИБ, описанные, например, в [1].

Они включают, в частности, вероятностные, графические, имитационные, игровые методы и модели описания.

Внутреннюю структуру информационной системы (ИС) целесообразно представлять в виде графа, в котором вершины являются элементами сети, а ребра (дуги) — средствами взаимодействия. Каждый из этих элементов может быть описан количественно в функции времени, причем оценки зависят от поставленной задачи. Например, для оптимизации загрузки сети наиболее эффективными могут быть потоки информации по каждой из дуг как средние по времени за заданный временной интервал, пиковые нагрузки, размеры информационных сообщений (максимальные, минимальные, средние за интервал оценивания), размеры буферной памяти в узлах сети, время задержки (ожидание связи), потери информации и т.д. Нас в данном случае интересуют угрозы безопасности. Оценки в данном случае могут быть следующих типов:

— вероятность несанкционированного доступа к информационным ресурсам от произвольного размещения нарушителя (одиночный или множественный вариант) в функции времени;

— стоимость однократного нарушения по простейшему варианту «одиночное нарушение — одиночный пункт нападения», также в функции времени;

— затраты на восстановление ущерба от нарушения по предыдущему варианту.

Введем следующие обозначения:

— $P(X_{IJ}, t)$ — вероятность успешной атаки I-го нарушителя на J-й элемент информационной системы;

— $C(X_{IJ}, t)$ — стоимость ущерба от однократного нападения в тех же координатах;

— $З(X_{IJ}, t)$ — стоимость восстановления информационной системы после нарушения ИБ.

Как видно из обозначений, все приведенные оценки являются функциями времени. Описываемые ими процессы являются случайными, причем нестационарными. Можно отметить их некоторые особенности. В частности, внутренние и внешние взаимодействия в информационных системах можно рассматривать как простейшие стационарные случайные процессы с равномерной загрузкой и равномерной плотностью распределения, не зависящей от времени. Это примитивная модель, не учитывающая реальной суточной загрузки сети, особенно в нештатных (пиковых) режимах, но она может быть использована в качестве первичной оценки, особенно по максимуму одного из анализируемых параметров.

Все количественные оценки имеют жесткую привязку к информационным объектам и зависят от множества внешних и внутренних факторов.

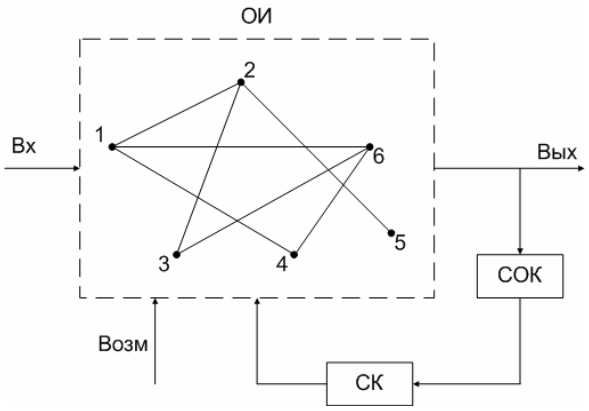


Рис. 1. Структура информационной системы

Внутренние — топология сети, режимы работы легальных пользователей (включая операционные системы, дополнительное программное обеспечение, режимы суточной работы, взаимодействие с другими пользователями и с внешней средой, включая Интернет). Внешние — количество внешних связей, режимы работы с ними. Большие проблемы создает новая услуга — Wi-Fi (Wi-MAX), которая серьезно снижает безопасность как сети, так и ее пользователей.

Кроме того, в качестве количественной оценки могут быть использованы показатели трафика (потоки информации, задержки, потери — все также в функции времени).

Обобщенная структура информационной системы приведена на рис. 1.

Здесь обозначено: ОИ — объект информатизации (собственно информационная система) с подсистемами, обозначенными цифрами и соединенными каналами связи; Вх и Вых — вход и выход обобщенного объекта информатизации; Возм — возмущения (в простейшем случае это помехи); СОК — система оперативного анализа и контроля; СК — система коррекции.

Для более корректного описания представим информационную систему в виде графа, в котором вершины представляют собой автономные объекты, имеющие некоторые информационные ресурсы и могущие взаимодействовать с другими такими же объектами. Граф приведен внутри ОИ. Под объектами в зависимости от глубины детализации могут быть персональные компьютеры или приравниваемые к ним аппаратные средства, локальные сети (LAN), корпоративные сети (MAN) с включаемым коммутационным оборудованием и стандартным оборудованием связи.

Каждый из выделенных объектов может иметь свои взаимодействия в зависимости от структуры системы. Не обязательно граф внутренних взаимодействий должен быть полносвязным (каждая вершина связана с остальными и образует при этом полный граф), просто в системе взаимодействий это учитывается в матрице задержек или потерь информации.

При принятых допущениях можно составить *матрицу взаимодействий* $R_{IJ}(t)$ размером $N \times N$, состоящую из элементов $\alpha_{IJ}(t)$, где N — количество узлов анализируемой ИС, $\alpha_{IJ}(t)$ — весовой коэффициент, определяемый в зависимости от типа решаемой задачи. Матрица имеет вид, приведенный на рис. 2. По матрице можно решать множество прикладных задач, связанных с определением $\alpha_{IJ}(t)$.

$$
\begin{vmatrix}
\alpha_{11}(t)\ \alpha_{12}(t)\ \alpha_{13}(t)\ \ldots\ldots\ldots\ldots\ldots\ldots\alpha_{1N}(t) \\
\alpha_{21}(t)\ \alpha_{22}(t)\ \alpha_{23}(t)\ \ldots\ldots\ldots\ldots\ldots\ldots\alpha_{2N}(t) \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\alpha_{N1}(t)\ \alpha_{N2}(t)\ \alpha_{N3}(t)\ \ldots\ldots\ldots\ldots\ldots\ldots\alpha_{NN}(t)
\end{vmatrix}
$$

Рис. 2. Матрица взаимодействий в информационной системе

Предположим, в качестве количественной оценки взят показатель удельного трафика $\alpha_{IJ}(t) = I(t)/T$, где T — время анализа. Тогда можно поставить следующие задачи (их список может быть дополнен).

1. Оптимизация трафика по выделенной сети по одному из возможных критериев: максимум суммарного количества переданной информации при существующих ограничениях по каждому из направлений.

2. Минимум потерь при заданных ограничениях на удельный трафик по каждому из направлений.

3. Минимизация времени задержки по всему графу или его фрагментам.

Возможны другие количественные показатели $\alpha_{IJ}(t)$:

а) вероятность нарушения ИБ по ребру IJ $p^{H}_{IJ}(t)$. В простейшем случае она может приниматься как стационарный процесс [2, 3]. Как альтернатива, может рассматриваться вероятность безопасной работы:

$$p^{Б}_{IJ}(t) = 1 - p^{H}_{IJ}(t). \qquad \textbf{(1)}$$

Здесь должны работать байесовские оценки для условных и безусловных событий.

Обозначим через $P_i(I, t)$ уязвимость i-го информационного ресурса объёма I. Очевидно, вероятность устойчивого существования информации уменьшается со временем:

$$P_i(I, t_2) \le P_i(I, t_1)\big|_{t2>t1}. \qquad \textbf{(2)}$$

Введём некоторую защиту R; соответствующая оценка вероятности равна $P_i^R(I,t)$. Исходя из общецелевого критерия, вероятность устойчивости информации при этом не уменьшается:

$$P_i^R(I, t) \ge P_i(I, t), \qquad \textbf{(3)}$$

где $P_i(I, t)$ — исходное состояние.

Если обозначить вероятность устойчивости после принятия нескольких способов защиты через $P_i^{\Sigma R}(I, t)$, то можно утверждать следующее [4, 5]:

1. Если профиль защиты информационного ресурса содержит несколько независимых операций, результирующая информационная безопасность не может быть ниже исходной.

2. Введение каждого дополнительного уровня защиты не может снижать информационную безопасность при условии, что уровни независимы.

Эти положения доказываются классическим аппаратом теории вероятности. Например, используются два уровня (способа) зашиты, причём вероятность взлома первого уровня равна $P_{H1}(t)$, а второго — $P_{H2}(t)$. Если способы защиты независимы, вероятность успешной атаки

$$P_{iB}(t) = P_{B1}(t) \cdot P_{B2}(t). \qquad \textbf{(4)}$$

Учитывая, что любая вероятность меньше единицы, выражение (4) подтверждает приведённые положения.

Если процедуры защиты зависимы, соответствующие байесовские оценки будут содержать условные вероятности:

$$P_B(t)=P_{B1}(t)\cdot P_{B2|B1}(t), \quad (5)$$

где $P_{B2|B1}(t)$ — условная вероятность зависимой атаки. Вполне может быть, что $P_{B2|B1}(t)=1$, и тогда безопасность сложного профиля защиты не повышается.

Для поиска функций $P_H(t)$ возможно натурное исследование объектов или априорное принятие законов распределения на основе классической теории вероятностей [3, 4]. Чаще всего используется распределение Пуассона:

$$P_H(t)=1-\exp(-rt), \quad (6)$$

где r — интенсивность нарушений.

Выражение (6) удобно использовать на практике при исследовании сложных информационных объектов с достаточно большим числом возможных источников нарушений: в этом случае показатели интенсивностей r_i просто суммируются, как это делается в теории надежности.

При наличии нескольких вариантов нарушений по одной цепочке информационной системы и при условии их независимости вероятности нарушений суммируются:

$$P_I(t)=\sum_{J=1}^{K}P_{IJ}(t). \quad (7)$$

Здесь K — количество независимых источников нарушений.

Из (7) следует, что одновременная атака нескольких независимых нарушителей (групповые атаки) очень опасна и со временем приводит к «успеху». В этой связи существенную опасность представляют так называемые «облачные» технологии [6];

б) стоимостные оценки. Обозначим затраты IJ-го участка информационной системы или отдельного участка доступа к информационному ресурсу через C_{IJ}. Тогда общая стоимость затрат на систему защиты определится как сумма всех показателей C_{IJ}. Более удобно вместо абсолютного показателя использовать относительную величину — *относительные затраты*:

$$\alpha_{IJ}=C_{IJ}/\sum_I\sum_J C_{IJ}\ . \quad (8)$$

Приведенный показатель удобно использовать при анализе и модернизации сетей. Легко отыскиваются дуги с наибольшими весами (назовем их критическими), после чего делаются попытки снижения соответствующих затрат.

Вернемся к первоначальной постановке задачи. Предположим, существует граф взаимодействий в информационной системе типа ОИ по рис. 1, а также матрица взаимодействий по рис. 2. При наличии коэффициентов α_{IJ}, в том числе в функции времени, на плоской модели безопасности (матрица взаимодействий) возможны задачи *оптимальных взаимодействий*. При этом главное — выбор критерия оптимальности. Это ключевая проблема, которая часто неправильно интерпретируется на практике.

Возможны следующие критерии.

1. Обеспечение минимальной вероятности нарушения ИБ при ограничениях по стоимости совокупных затрат (затраты на оборудование, программное обеспечение, обучение персонала, дополнительные затраты на премии за безопасность и т.д.).

2. Минимизация затрат на безопасность при соблюдении существующих нормативов с учетом времени.

Возможны и другие критерии, особенно в сферах, сопряженных с техногенными ситуациями. Например, максимальная безопасность технического объекта, процесса, финансовой системы, системы обеспечения жизнедеятельности и т.д.

Матрица взаимодействий по рис. 2 является плоской моделью информационных взаимодействий. С позиций математики она описывает прямые взаимодействия объектов, т.е. без промежуточных пунктов ретрансляции, коммутации и т.д. Кроме того, по графу ОИ возможно решение более сложных задач взаимодействия через промежуточные вершины графа, т.е. маршрутизация взаимодействий. На плоских моделях существуют алгоритмы Дийкстры, Форда – Фалкерсона и т.д. [7 – 10].

Авторами предложен трехмерный вариант матрицы взаимодействий. Он обобщает плоскую модель взаимодействий. В плоской модели коэффициенты α_{IJ} являются числовыми эквивалентами непосредственных взаимодействий между объектами информационной системы или этапами взаимодействия. Трехмерная модель учитывает опосредованные взаимодействия. На языке теории графов трехмерные матрицы описывают маршруты различной длины. Так, второй слой (вторая плоская матрица) описывает взаимодействия маршрутов длины 2, т.е. через одно промежуточное звено; третья плоская матрица представляет маршруты длины 3 и т.д. При этом траектория маршрутизации становится трехмерной при добавлении третьей координаты — длина маршрута L. Предложенные выше выражения легко обобщаются на трехмерный вариант. При этом границы по третьей координате могут быть четко ограничены, что вписывается в стандарты TCP/IP. Достаточно учесть поправки в заголовок пакета IP по ограничению числа ретрансляций: это и есть границы третьей координаты.

Предложенный алгоритм был использован на компьютерных моделях и на некоторых конкретных информационных объектах. В отличие от плоских моделей, он обладает большей гибкостью, большей результативностью и обеспечивает лучшие конечные результаты с учетом особенностей конкретного объекта и его функционирования.

Библиографический список

1. Шахов, В. Г. Методы и алгоритмы анализа и планирования информационной безопасности: опыт использования / В. Г. Шахов // Безопасность информационных технологий. – 2005. – № 4. – 102 с.

2. Кендалл, М. Статистические выводы и связи / М. Кендалл, А. Стьюарт. – М. : Наука, 1973. – 900 с.

3. Бендат, Д. С. Измерение и анализ случайных процессов / Д. С. Бендат, А. Дж. Пирсол. – М. : Мир, 1971. – 390 с.

4. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. – М. : ДМК Пресс, 2010. – 544 с.

5. Майстренко, В. А. Безопасность информационных систем и технологий / В. А. Майстренко, В. Г. Шахов. – Омск : ОмГТУ, 2006. – 232 с.

6. Гюнтер, Е. В.Облачные технологии и проблемы их безопасности / Е. В. Гюнтер, Н. Н. Нарутта, В. Г. Шахов // Ом-

ский научный вестник. Сер. Приборы, машины и технологии. — 2013. — № 3. — С. 278—282.

7. Определение оптимального маршрута перевозки грузов [Электронный ресурс] : электрон. учеб. пособие / Шахов В. Г., Афоничев Н. Ю. ; Омский гос. ун-т путей сообщения ; каф. «Автоматика и системы управления». — Омск : ОмГУПС, 2012. — 1 электрон. опт. диск (CD-ROM).

8. Шахов, В. Г. Игровые и топологические модели информационной безопасности / В. Г. Шахов, А. В. Морозов, А. П. Тиунов, А. Н. Громов // Известия Транссиба. — 2014. — № 3(19). — 158 с.

9. Шахов, В. Г. Введение в информационные системы и телекоммуникации / В. Г. Шахов. — Омск : ОмГУПС, 2001. — 87 с.

10. Заде, Л. Понятие лингвистической переменной и его применение к принятию приближенных решений / Л. Заде. — М. : Мир, 1976. — 446 с.

ГРОМОВ Андрей Николаевич, аспирант кафедры автоматики и систем управления.
ТИУНОВ Артём Павлович, аспирант кафедры автоматики и систем управления.
ФОМЕНКО Мария Сергеевна, магистрант гр. 24-И института автоматики, телекоммуникаций и информационных технологий.
ШАХОВ Владимир Григорьевич, кандидат технических наук, профессор кафедры автоматики и систем управления.

Адрес для переписки: shahovvg@mail.ru

Статья поступила в редакцию 05.03.2015 г.

УДК 004.7:056.5

А. В. ЛЕОНОВ

Омский государственный технический университет

ИНТЕРНЕТ ВЕЩЕЙ: ПРОБЛЕМЫ БЕЗОПАСНОСТИ

Исследования в области безопасности Интернета вещей все чаще привлекают внимание научных кругов. В данном исследовании рассматриваются три ключевых требования безопасности с акцентом на системы Интернета вещей: аутентификация, конфиденциальность и управление доступом. Акцентируется внимание на вопросах безопасности, не решенных к настоящему моменту, а также рассматриваются проблемы и будущие тенденции в области Интернета вещей.

Ключевые слова: Интернет вещей, безопасность, аутентификация, конфиденциальность, управление доступом.

Введение. Интернет вещей (Internet of Things, IoT) — это концепция и парадигма, которая рассматривает повсеместно распространяющееся присутствие различных физических объектов («вещей») в окружающей среде. Термин «Интернет вещей» определен как динамическая глобальная сетевая инфраструктура с возможностью самонастройки на основе стандартных и совместимых протоколов связи, где физические и виртуальные «вещи» имеют идентификаторы, физические атрибуты, используют интеллектуальные интерфейсы и интегрируется в информационную сеть [1].

В течение последнего десятилетия Интернет вещей проникал в нашу жизнь тихо и постепенно, прежде всего благодаря наличию систем беспроводной связи (например, RFID, Wi-Fi, 4G, IEEE 802.15.x), которые все чаще используются в качестве движущей силы для развития технологии интеллектуального контроля и управления приложениями [2].

Концепция IoT включает в себя множество различных технологий, услуг, стандартов и воспринимается как краеугольный камень на рынке информационно-коммуникационных технологий (ИКТ) по крайней мере на ближайшие десять лет.

С логической точки зрения, система IoT может быть представлена как совокупность совместно взаимодействующих интеллектуальных устройств. С технической точки зрения, IoT может использовать различные пути обработки данных, коммуникации, технологии и методологии, основываясь на их целевом предназначении. Например, система IoT может использовать возможности беспроводной сенсорной сети (WSN), которая собирает экологически значимую информацию об окружающей среде [3].

Высокий уровень неоднородности в сочетании с широкой гаммой систем IoT, как ожидается, увеличит число угроз безопасности владельцев устройств, которые все чаще используются для взаимодействия людей, машин и вещей в любой вариации. Традиционные меры обеспечения безопасности и соблюдения конфиденциальности не могут быть применены к технологиям IoT, в частности, из-за их ограниченной вычислительной мощности. Кроме того, большое количество подключенных устройств порождает проблему масштабируемости. В то же время для достижения признания со стороны пользователей необходимо в обязательном порядке обеспечить соблюдение безопасности, конфиденциальность и модели доверия, подходящие для контекста IoT [4—6]. Для предотвращения несанкционированного доступа пользователей (то есть людей и устройств) к системе должны использоваться механизмы аутентификации и авторизации, гарантирована безопасность, конфиденциальность и целостность персональных данных. Относительно персональных данных пользователей и информации должны обеспечиваться защита и конфиденциальность, прежде всего потому, что устройства имеют к ней доступ и способны ей управлять (например, сведения о привычках пользователей). Наконец, доверие

(надёжность, англ. Trust) — это основная проблема, поскольку IoT-среда характеризуется различными типами устройств, которые должны обрабатывать данные в соответствии с потребностями и правами пользователей.

Обратим внимание, что адаптация и самовосстановление играют ключевую роль в IoT инфраструктурах, которые должны быть в состоянии противостоять неожиданным изменениям в окружающей среде. Соответственно, к вопросам конфиденциальности и безопасности следует относиться с высокой степенью гибкости. Наряду с традиционными решениями для обеспечения безопасности необходимо использование специальных механизмов, встроенных в сами устройства с целью оперативного диагностики, изоляции и профилактики нарушений [7].

Аутентификация и конфиденциальность. Что касается аутентификации, подход, представленный в [8], предусматривает использование настраиваемого пользователем механизма инкапсуляции, а именно протокол прикладного уровня для IoT под названием — «интеллектуальная служба обеспечения безопасности» (англ. Intelligent Service Security Application Protocol). Он сочетает в себе кросс-платформенные связи с шифрованием, подписью и аутентификацией для повышения эффективности разработки приложений IoT путем создания системы защищенной связи между различными вещами.

В работе [9] представлена первая полностью реализованная двусторонняя схема проверки подлинности для IoT на основе существующих стандартов, в частности, протокол датаграмм безопасности транспортного уровня (англ. Datagram Transport Layer Security, DTLS), который располагается между транспортным и прикладным уровнями. Эта схема основана на криптографическом алгоритме RSA и предназначена для IPv6 с использованием стандарта 6LoWPANs (англ. IPv6 over Low power Wireless Personal Area Networks) [10]. Анализ результатов, основанных на реальных системах IoT, показывает, что такая архитектура обеспечивает целостность сообщения, конфиденциальность, энергоэффективность, низкие значения задержки пакетов и нагрузки на память.

Относительно конфиденциальности и целостности в [11] приведен анализ того, как существующие системы управления ключами могут быть применены в контексте IoT. Это позволяет классифицировать протоколы систем управления ключами (англ. Key Management System, KMS) по четырем основным категориям: структура пула ключей, математическая база, механизм взаимодействия и структура открытого ключа. В работе [12] авторы утверждают, что большинство протоколов KMS не подходят для IoT. Однако протоколы KMS пригодны для сценариев, в которых вычислительные мощности являются довольно низкими по сравнению с использованием криптографии с открытым ключом (англ. Public Key Cryptography, PKC). Но для таких схем необходимо введение нескольких контрмер для управления устройством аутентификации и во избежание MITM-атаки (англ. Man In The Middle).

Более практичный подход [13] предлагает модель передачи со схемами шифрования подписи, в которой рассматриваются требования безопасности IoT (т.е. анонимность, надежность и устойчивость к атакам) посредством ONS-запросов (англ. Object Naming Service). Однако, с точки зрения устойчивости к атакам, результаты модели передачи данных являются очень слабыми в связи с использованием шифрования на базе «точка—точка» (англ. hop-by-hop).

По-прежнему отсутствует уникальное и четко определенное решение, которое может гарантировать конфиденциальность в IoT. В этом контексте много усилий было приложено для WSN (англ. WSN — Wireless Sensor Network) [14, 15], но, несмотря на это, возникает несколько вопросов:

— Являются ли предложения для WSN легко адаптируемыми к среде IoT, учитывая как неоднородность устройств, так и различия в области применения?

— Как и на каком сетевом уровне осуществляется аутентификация?

— Реально ли использовать традиционные механизмы безопасности (например, алгоритмы шифрования) или лучше начать с новых решений?

— Как обрабатывать разные ключи?

— Какой вид распределения ключевого механизма является наиболее подходящим?

— Как обеспечить непрерывный механизм проверки целостности для того, чтобы сделать систему более устойчивой к атакам злоумышленников?

Совсем недавно началась работа по решению этих вопросов. Например, протокол аутентификации для IoT, представленный в [16], использует легкий метод шифрования, основанный на операции XOR.

В рамках WSN аутентификация пользователя и схема согласования ключа для гетерогенных беспроводных сенсорных сетей также предложена, например, в [17]. Это решение позволяет удаленному пользователю безопасно договориться о сеансовом ключе с сенсорным узлом с помощью протокола распределения ключей. Таким образом, он обеспечивает взаимную аутентификацию между пользователями, сенсорными узлами и шлюзовыми узлами (англ. gateway node, GWN). Для того чтобы применить такую схему для архитектуры с ограниченными ресурсами, используются только простые хэш и XOR вычисления.

Метод проверки подлинности и контроль доступа, представленный в [18], направлен на создание ключа сеанса с применением эллиптической криптографии (англ. Elliptic Curve Cryptography, ECC). Кроме того, предложен механизм защиты данных в облачных хранилищах, основанный на сочетании «классической» проблемы Диффи—Хеллмана и проблемы дискретного логарифмирования в группе точек эллиптической кривой. Отмечается, что протокол, основанный на эллиптических кривых, имеет небольшой размер ключа без ущерба криптостойкости, что делает эллиптическую криптографию привлекательной для использования в тех областях, где существуют проблемы из-за ограничения памяти и вычислительных мощностей.

Контроль доступа. Управление доступом относится к разрешениям в области использования ресурсов, предназначенных для различных субъектов в сети IoT. В [19] определены два субъекта: владельцы данных и сборщики данных. Пользователи и вещи, как держатели данных, должны позволять передавать только сведения, которые необходимы для выполнения конкретной задачи. В то же время сборщики данных должны уметь идентифицировать или подтвердить подлинность (аутентифицировать) пользователей вещей как законных владельцев данных, от которых она собирается.

В IoT мы имеем дело с обработкой потоковых, а не дискретных данных, как в традиционных системах. Основные проблемы в этом контексте отно-

сятся к производительности и временным ограничениям. В частности, поток данных интенсивнее, чем в традиционных системах управления базами данных (СУБД). Несколько работ посвящено этим аспектам.

В [20] внимание сосредоточено на уровне, ответственном за получение и хранение информации. Большое количество узлов авторизованных пользователей использует широкий спектр различных типов данных соответствующих уровням конфиденциальности и безопасности. Поэтому в работе представлена иерархическая схема управления доступом для этого уровня. Схема учитывает ограниченную вычислительную мощность и емкость устройства хранения. Каждому пользователю и/или узлу дается только один ключ; другие необходимые ключи получены с помощью детерминированного алгоритма деривации ключа (англ. deterministic key derivation algorithm), повышая уровень безопасности (так как обмен ключей ограничен) и сокращая затраты на хранение для множества узлов.

В [21] разработана архитектура безопасности, которая направлена на обеспечение целостности и конфиденциальности данных. Механизм основан на алгоритме FT-RC4 (является расширением RC4), который представляет собой потоковый шифр.

Статья [22] фокусируется на повышении производительности и масштабируемости СУБД. Подход, который устраняет проблему аутентификации внешних потоков данных с использованием непрерывной проверки подлинности в потоках данных (англ. Continuous Authentication on Data Streams, CADS), можно найти, например, в [23]. В этих работах предполагается наличие поставщика услуг, который собирает данные от одного или нескольких владельцев вместе с информацией аутентификации и при этом одновременно обрабатывает запросы множества клиентов. Поставщик услуг возвращает клиентам результаты запросов, а также информацию о проверке, что позволяет им проверить подлинность и полноту полученных результатов на основе информации аутентификации, предоставленной владельцем данных.

В публикации [24] внимание также фокусируется на аутсорсинге данных. В частности, из-за большого количества потоковых данных компании могут не приобретать ресурсы, необходимые для развертывания систем управления потоками данных (англ. Data Stream Management Systems, DSMS). Предлагается делегировать хранение и обработку потока специализированному третьему лицу с сильной инфраструктурой DSMS. Появляется вопрос доверия: третье лицо может действовать злонамеренно, например, с целью увеличения своей прибыли. Решение заключается в том, чтобы принять метод для аутентификации потока так, чтобы клиенты могли проверить целостность и актуальность полученных от сервера данных. При этом метод должен удовлетворять требованиям IoT устройств, характеризующихся ограниченными ресурсами с точки зрения энергопотребления, вычислительной мощности и ЗУ.

Главными проблемами, связанными с контролем доступа в сценарии IoT, являются следующие вопросы:

— Как гарантировать права доступа в среде, в которой не только пользователи, но и вещи могут взаимодействовать с системой?

— Какой подход использования наиболее эффективен: централизованный, распределенный или полураспределенный для управления масштабируемой IoT архитектурой?

— Как обрабатывать огромный объем передаваемых данных (т.е. в виде потока данных)?

Что касается идентификации, одним из главных изменений сегодня является увеличение мобильности портативных и мощных беспроводных устройств. Для решения этой проблемы требуется доработать архитектуру в части правил именования, адресации, кроме того необходимо развитие определенной структуры управления данными для IoT. Лишь в единичных работах предлагается решение этой проблемы. Без ответа остаются следующие проблемные аспекты:

— для управления контролем доступа IoT система может осуществлять регистрацию пользователей и вещей, для чего необходимо наличие соответствующего полномочного органа для выдачи удостоверений или сертификатов;

— пользователи/вещи должны иметь возможность предоставить учетные данные/сертификаты системе IoT для того, чтобы взаимодействовать с другими авторизованными/разрешенными устройствами;

— определение конкретных ролей и функций в рамках IoT для управления процессами авторизации.

Что касается затронутых вопросов, несколько новых решений недавно были предложены. В [25] представлена схема авторизации для устройств с ограниченными ресурсами, которая сочетает в себе технологии физически неклонируемых функций (англ. Physical Unclonable Functions, PUFS) со встроенным модулем идентификации абонента (англ. Subscriber Identity Module, eSIM). Первая обеспечивает недорогие, безопасные секретные ключи с защитой от взлома для M2M (англ. MACHINE-to-MACHINE) устройств. Вторая обеспечивает мобильную связь, гарантирующую масштабируемость, совместимость и соответствие протоколам безопасности.

Групповая передача (англ. Multicast) рассмотрена в [26], где используется общий секретный ключ, обозначенный как групповой, общий для нескольких конечных точек обмена данными. Такие ключи управляются и распространяются на основе централизованного подхода. Заметим, что такой механизм снижает накладные расходы (количество вычислительных ресурсов) и сетевой трафик из-за изменений состава в группах, вызванных пользовательскими соединениями, как это происходит в IoT. Такой протокол может быть применен в двух соответствующих сценариях: 1) безопасная агрегация данных в IoT и 2) коммуникация в автомобильных одноранговых сетях VANETs (англ. Vehicle-to-Vehicle, V2V).

Заключение. Распространение услуг IoT требует чтобы были гарантированы безопасность и конфиденциальность. Проведенный обзор публикаций и работ наглядно демонстрирует, насколько много остается нерешенных проблем, проливает свет на направления исследований в области безопасности IoT. До сих пор не сформулирована единая концепция относительно требований безопасности и конфиденциальности в такой разнородной среде с применением различных технологий и стандартов связи. Подходящие решения необходимо разработать и реализовать. Они должны быть независимыми от платформ и позволять гарантировать контроль доступа и конфиденциальность пользователей и вещей, надежность среди устройств и пользователей, соблюдение определенных политик безопасности

и конфиденциальности. Требуется проведение научно-исследовательской работы по направлению обеспечения безопасности IoT в мобильных устройствах, которое получает все более широкое распространение сегодня. Много усилий было (и еще будет) приложено мировым научным сообществом для решения существующих нерешенных задач. При этом в процессе работы появится множество новых вопросов, с которыми только предстоит столкнуться. Данная статья будет полезна в выборе дальнейших направлений исследований и поспособствует массовому развертыванию систем IoT в реальном мире.

Библиографический список

1. Internet of Things Global Standards Initiative [Электронный ресурс]. — Режим доступа : http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx (дата обращения: 05.02.2015).

2. Алгулиев, Р. Ш. Интернет вещей / Р. Ш. Алгулиев, Р. Ш. Махмудов // Информационное общество. — 2013. — № 3. — С. 42—48.

3. L. A. Grieco, M. B. Alaya, T. Monteil, K. K. Drira, Architecting information centric ETSI-M2M systems, in: IEEE PerCom, 2014.

4. R. H. Weber, Internet of things - new security and privacy challenges, Comput. Law Secur. Rev, Jan. 2010, Vol. 26, № 1, pp. 23—30.

5. H. Feng, W. Fu, Study of recent development about privacy and security of the internet of things, in: 2010 : International Conference on Web Information Systems and Mining (WISM), Sanya, 2010, pp. 91—95.

6. R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Networks, 2013, Vol. 57, № 10, pp. 2266—2279.

7. S. Babar, A. Stango, N. Prasad, J. Sen, R. Prasad, Proposed embedded security framework for internet of things (iot), in: 2011 : 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology (VITAE), Chennai, India, 2011, pp. 1—5.

8. Y. Zhao, Research on data security technology in internet of things, in: 2013 : 2nd International Conference on Mechatronics and Control Engineering (ICMCE), Dalian, China, 2013, pp. 1752—1755.

9. T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, G. Carle, Dtls based security and two-way authentication for the internet of things, Ad Hoc Networks, 2013, Vol. 11. № 8, pp. 2710—2723.

10. M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, M. Dohler, Standardized protocol stack for the internet of (important) things, IEEE Commun. Surv. Tutorials, 2013, Vol. 15, № 3, pp. 1389—1406.

11. R. Roman, C. Alcaraz, J. Lopez, N. Sklavos, Key management systems for sensor networks in the context of the internet of things, Comput. Electrical Eng., 2011, Vol. 37, № 2, pp. 147—159.

12. W. Du, J. Deng, Y. Han, P. Varshney, J. Katz, A. Khalili, A pairwise key predistribution scheme for wireless sensor networks, ACM Trans. Inf. Syst. Secur. (TISSEC), 2005, Vol. 8, № 2, pp. 228—258.

13. Z.-Q. Wu, Y.-W. Zhou, J.-F. Ma, A security transmission model for internet of things, Jisuanji Xuebao/Chin. J. Comput., 2011, Vol. 34, № 8, pp. 1351—1364.

14. Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, Alberto Coen-Porisini, Security, Privacy & Trust in Internet of Things: the road ahead, Computer Networks (Elsevier), 2015, Vol. 76, pp. 146—164.

15. Богданов, И. А. Анализ особенностей обеспечений сетевой безопасности во всепроникающих сенсорных сетях / И. А. Богданов, А. Е. Кучерявый // Информационные технологии и телекоммуникации. — 2013. — № 2 (2). — С. 4—12.

16. J.-Y. Lee, W.-C. Lin, Y.-H.Huang, A lightweight authentication protocol for internet of things, in: 2014 : International Symposium on Next-Generation Electronics (ISNE), Kwei-Shan, 2014, pp. 1—2.

17. M. Turkanovi, B. Brumen, M. Holbl, A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion, Ad Hoc Networks, 2014, Vol. 20, pp. 96—112.

18. N. Ye, Y. Zhu, R.-C. b. Wang, R. Malekian, Q.-M. Lin, An efficient authentication and access control scheme for perception layer of internet of things, Appl. Math. Inf. Sci., 2014, Vol. 8, № 4, pp. 1617—1624.

19. A. Alcaide, E. Palomar, J. Montero-Castillo, A. Ribagorda, Anonymous authentication for privacy-preserving iot targetdriven applications, Comput. Secur., 2013, Vol. 37, pp. 111—123.

20. J. Ma, Y. Guo, J. Ma, J. Xiong, T. Zhang, A hierarchical access control scheme for perceptual layer of iot, Jisuanji Yanjiu yu Fazhan, Comput. Res. Dev., 2013, Vol. 50, № 6, pp. 1267—1275.

21. M. Ali, M. ElTabakh, C. Nita-Rotaru, FT-RC4: A Robust Security Mechanism for Data Stream Systems, Tech. Rep. TR-05-024, Purdue University, Nov. 2005, pp. 1—10.

22. M. A. Hammad, M. J. Franklin, W. Aref, A. K. Elmagarmid, Scheduling for shared window joins over data streams, in : Proceedings of the 29th International Conference on Very Large Data Bases (VLDB), Berlin, Germany, 2003, pp. 297—308.

23. S. Papadopoulos, Y. Yang, D. Papadias, Continuous authentication on relational data streams, VLDB Journal, 2010, Vol. 19, № 1, pp. 161—180.

24. S. Papadopoulos, G. Cormode, A. Deligiannakis, M. Garofalakis, Lightweight authentication of linear algebraic queries on data streams, in : Proceedings of the 2013 ACM SIGMOD International Conference on Management of Data (SIGMOD), New York, USA, 2013, pp. 881—892.

25. A. Cherkaoui, L. Bossuet, L. Seitz, G. Selander, R. Borgaonkar, New paradigms for access control in constrained environments, in: 2014 : 9th International Symposium on Reconfigurable and Communication-Centric Systems-on-Chip (ReCoSoC), Montpellier, 2014, pp. 1—4.

26. L. Veltri, S. Cirani, S. Busanelli, G. Ferrari, A novel batch-based group key management protocol applied to the internet of things, Ad Hoc Networks, 2013, Vol. 11, № 8, pp. 2724—2737.

ЛЕОНОВ Алексей Викторович, начальник сектора Internet-технологий Центра телекоммуникаций и вычислительной техники; соискатель по кафедре средств связи и информационной безопасности.
Адрес для переписки: kot@omgtu.ru

Статья поступила в редакцию 28.03.2015 г.

ВИКТОРУ ИЛЬИЧУ ПОТАПОВУ — 80 ЛЕТ

8 июля 2015 года исполняется 80 лет ПОТАПОВУ ВИКТОРУ ИЛЬИЧУ — доктору технических наук, профессору, заслуженному деятелю науки и техники Российской Федерации, действительному члену Международной академии наук высшей школы и Международной академии информатизации, проректору по научной работе Омского политехнического института (1978–1985 гг.), заведующему кафедрой информатики и вычислительной техники (с 1972 г.).

Потапов В. И. родился 8 июля 1935 г. в г. Омске. Окончил радиофизический факультет Томского государственного университета по специальности радиофизика и электроника.

После окончания университета, с 1961 по 1965 г., работал инженером в СКБ предприятия п/я № 2 Министерства радиопромышленности СССР, в конструкторско-технологическом институте, где занимался разработкой специализированных вычислительных устройств для систем управления подвижными объектами и технологическими процессами. С 1965 по 1968 гг. обучался в очной аспирантуре на факультете систем управления летательных аппаратов в Московском авиационном институте им. С. Орджоникидзе.

В 1969 г. В. И. Потапов защитил кандидатскую диссертацию, в 1972 г. утвержден в ученом звании доцента. В 1976 г. на основании защиты докторской диссертации в Томском государственном университете Виктору Ильичу была присуждена ученая степень доктора технических наук, а в 1977 г. ему присвоено ученое звание профессора.

С 1968 г. В. И. Потапов работает в Омском государственном техническом университете. Им основана кафедра «Электронные вычислительные машины», начавшая впервые в Омске подготовку инженеров по вычислительной технике, организованы общеинститутский вычислительный центр и отраслевая научно-исследовательская лаборатория «Автоматизация проектирования АСУ», создан научный центр «Информатика» для разработки региональной программы информатизации Омской области.

Будучи проректором по научной работе (1977–1985 гг.), разработал и внедрил с коллегами в ОмГТУ систему учебно-научно-производственных комплексов. Разработанная на ее основе эффективная система управления научными исследованиями позволила ОмГТУ в 1981–1984 гг. войти в число ведущих вузов России в области научной деятельности, а также была удостоена в 1982 г. серебряной медали ВДНХ, а в 1983 г. — признана Минвузом РСФСР лучшей в Российской Федерации и отмечена дипломом I степени.

Все научно-исследовательские работы, проводимые под научным руководством В. И. Потапова, выполнялись по научно-техническим программам ГКНТ СССР, программам Минвуза РСФСР и СССР и по отраслевым программам, а в последнее время — по единому заказ-наряду и грантам Минобрнауки РФ на фундаментальные исследования.

К основным результатам научно-исследовательских работ можно отнести следующие:

— созданы основы схемотехники, информационной технологии контроля и диагностики многофункциональных элементов с кодовой перестройкой логики в пороговом базисе, схемотехника логически запоминающих структур с перестройкой логики на базе цилиндрических магнитных доменов, нашедших применение в специализированных вычислительных устройствах. Разработки по этому направлению защищены 32 авторскими свидетельствами на изобретение. Опубликована монография «Схемотехника и контроль элементов пороговой логики»;

— созданы теоретические основы и новые информационные технологии таблично-алгоритмических вычислений функций в ЭВМ, на базе которых создано и внедрено большое число оригинальных вычислительных алгоритмов и цифровых вычислительных структур для воспроизведения широкого класса функций. По результатам этих научных исследований опубликована монография «Таблично-алгоритмические вычисления функций в ЭВМ» и многочисленные статьи, а новые технические решения в рамках этого направления защищены 14 авторскими свидетельствами;

— созданы новые эффективные программно-имитационные комплексы моделирования вычислительных структур и вычислительных процессов для информационных технологий автоматизации проектирования АСУ реального времени, внедренные в ряде организаций Минприбора СССР. Все пакеты прикладных программ сданы в государственный и отраслевой фонды алгоритмов и программ и доступны для широкого круга специалистов.

Поставлены и решены новые задачи оптимизации резервированных систем, внесшие существенный научный вклад в теорию надежности. В рамках этого направления впервые решены оптимизационные задачи резервирования восстанавливаемых и невосстанавливаемых систем со скользящим резервом, интенсивность отказов элементов которых является функцией времени; оригинальные задачи оптимального управления подвижными системами и игровые задачи типа «нападение – зашита» между системами. Все решения доведены до рабочих алгоритмов, легко используемых на практике. По данному направлению опубликован ряд статей в центральных журналах и издана монография «Новые задачи оптимизации резервированных систем».

Под научным руководством В. И. Потапова проведены фундаментальные исследования по теме «Разработка методов и создание средств автоматизации исследований надежности и безопасности сложных систем управления техническими объектами». Работа направлена на создание новой информационной технологии, базирующейся на превышающих мировой уровень методах инструментальных и программных средств автоматизированной имитации неисправностей в действующей системе, и проведение испытаний на надежность и безопасность систем управления в энергетике, нефтехимии, космических исследованиях. Основные компоненты разработки и способы реализации защищены четырьмя авторскими свидетельствами. Написана монография «Методы и средства автоматизированного исследования последствий неисправностей и оценки надежности цифровых устройств».

В течение последних пятнадцати лет на основании фундаментальных исследований впервые в мире созданы основы теории надежности и технической диагностики искусственных нейронных сетей нейрокомпьютерных систем в рамках приоритетного развития новых поколений ЭВМ в XXI веке. По результатам научных исследований в данном направлении за последние годы профессором В. И. Потаповым опубликовано 49 статей, изданы три учебных пособия, два из которых — с грифом УМО, для магистрантов и студентов университета и пять монографий: «Основы технической диагностики искусственных нейронов и нейронных сетей», «Математические модели, методы и алгоритмы оптимизации надежности и технической диагностики искусственных нейронных сетей», «Теоретические основы диагностики и оптимизации надежности искусственных нейронных сетей», «Новые задачи прикладной теории надежности нейрокомпьютерных систем», «Модели для решения задач надежности искусственных нейронных систем».

В последние годы научную деятельность профессор В. И. Потапов сосредоточил на разработке моделей, алгоритмов и программного обеспечения для решения оптимизационных задач противоборства технических систем в конфликтных ситуациях. По результатам этих исследований опубликовано 12 статей, зарегистрировано в фондах алгоритмов и программ четыре программы для ЭВМ и написана монография «Противоборство технических систем в конфликтных ситуациях: модели и алгоритмы».

В целом по результатам научной и научно-методической деятельности опубликовано более 700 работ, включая 10 монографий, 25 учебных пособий для студентов вузов и 165 изобретений в области информатики и вычислительной техники, из которых 26 внедрены; в фондах алгоритмов и программ зарегистрировано более 30 программ для ЭВМ. Под его редакцией издано 12 межвузовских сборников научных трудов.

К научным исследованиям профессор В. И. Потапов широко привлекает студентов и аспирантов, которые неоднократно занимали призовые места на всероссийских конкурсах и олимпиадах. Многие результаты научных работ используются в учебном процессе при подготовке бакалавров и магистров по направлению «Информатика и вычислительная техника», инженеров-схемотехников по специальности «Вычислительные машины, комплексы, системы и сети», а также при обучении аспирантов.

Научную деятельность профессор В. И. Потапов сочетает с активной подготовкой инженерных и научных кадров. Он создал известную в России и за ее пределами научную школу и является членом научно-методических объединений Министерства образования и науки России по

специальности «Вычислительные машины, комплексы, системы и сети» и направлению «Информатика и вычислительная техника». Возглавляемая им кафедра информатики и вычислительной техники выпустила более 4000 инженеров-схемотехников; с сентября 1992 года она первой в городе Омске перешла на многоуровневую подготовку специалистов-бакалавров, а с 2006 г. — магистрантов в области информатики и вычислительной техники.

Через систему аспирантуры и соискательства профессор В. И. Потапов подготовил 22 кандидата наук, работающих на многих кафедрах технического университета и других вузов, в НИИ, КБ. Ученики профессора В. И. Потапова защитили 10 докторских диссертаций.

Профессор В. И. Потапов ведёт большую общественную работу. В 1990—1994 гг. являлся народным депутатом Омского областного Совета народных депутатов, где возглавлял постоянную комиссию по науке и образованию. В разные годы избирался председателем правления Омской областной организации Союза научных и инженерных организаций Российской Федерации, являлся членом координационного совета Союза НИО РФ, членом Центрального правления Российского НТО РЭС имени А. С. Попова, членом президиума Омского областного межведомственного совета по науке при областной администрации, председателем Омского территориального органа Всероссийского фонда образования, заместителем председателя и членом диссертационных советов в ОмГТУ, членом докторских диссертационных советов в университетах Новосибирска и Томска.

За успехи в научной и педагогической деятельности профессор В. И. Потапов имеет почётные грамоты, дипломы и благодарности Минвуза СССР, Минвуза РСФСР, ЦК ВЛКСМ, Омского городского Совета народных депутатов, Комитета по высшей школе России, Президиума Центрального совета ВОИР и других ведомств. Награждён знаком Минвуза СССР «За отличные успехи в работе», знаком «Изобретатель СССР», знаком Минсвязи СССР «Почётный радист СССР». За активную общественную деятельность удостоен знака ВНТО СССР «За активную работу в НТО», звания «Почётный член Российского НТО РЭС имени А. С. Попова».

Как выдающемуся ученому профессору В. И. Потапову присуждалась Государственная научная стипендия в области информатики и вычислительной техники.

В 1993 году Президентом Российской Федерации профессору В. И. Потапову присвоено почетное звание «Заслуженный деятель науки и техники Российской Федерации».

Коллеги по работе, друзья, ученики от всей души поздравляют Виктора Ильича с юбилеем и желают ему крепкого здоровья, долгих лет жизни, благополучия и дальнейших успехов в профессиональной деятельности!

Макаров Владимир Вячеславович,
декан факультета информационных технологий
и компьютерных систем ОмГТУ