Intellectual Technologies on Transport
No 1

Интеллектуальные технологии на транспорте
№ 1

Санкт-Петербург
St. Petersburg
2017

Интеллектуальные технологии на транспорте
№ 1, 2017

Сетевой электронный научный журнал, свободно распространяемый через Интернет.
Публикует статьи на русском и английском языках с результатами исследований и практических достижений в области интеллектуальных технологий и сопутствующих им научных исследований

Журнал основан в 2015 году

Учредитель и издатель

Федеральное государственное бюджетное образовательное учреждение высшего образования «Петербургский государственный университет путей сообщения Императора Александра I» (ФГБОУ ВПО ПГУПС)

Адрес редакции
190031 Санкт-Петербург, Московский пр., 9, ПГУПС
email: itt-pgups@yandex.ru, сайт: http://itt-pgups.ru/, редактор сайта Рогальчук В.В.

ISSN 2413-2527

Журнал зарегистрирован Федеральной службой по надзору в сфере связи и массовых коммуникаций, свидетельство ЭЛ № ФС77-61707 от 07 мая 2015 г.

Журнал зарегистрирован в Российском индексе научного цитирования (РИНЦ)

Intellectual Technologies on Transport
Issue № 1, 2017

Network electronic scientific journal, open access. It publishes articles in Russian and English with the results of research and practical achievements in the field of intelligent technologies and associated research

Founded in 2015

Founder and Publisher
Federal State Educational Institution of Higher Education
«Emperor Alexander I Petersburg State Transport University»

Adress
190031, St. Petersburg, Moskovskiy pr., 9, 2–108
email: itt-pgups@yandex.ru, http://itt-pgups.ru/, Site Editor: Rogalchuk V.V.

ISSN 2413-2527

The journal is registered by the Federal Service for Supervision of Communications and Mass Media, EL №FS77-61707 testimony from May 7, 2015

The journal is registered in the Russian Science Citation Index (RSCI)

Содержание

Contents

Эвристическая модель ликвидации нештатных ситуаций в эргатических системах управления

Смагин В. А.
Военно-космическая академия им. А. Ф. Можайского
Санкт-Петербург, Россия
va_smagin@mail.ru

Аннотация. **Предлагается модель ликвидации нештатной ситуации в работе эргатической (человеко-машинной) системы. Модель включает два этапа: предварительного обучения и тренировки операторов управления в лабораторных условиях; и непосредственной ликвидации операторами нештатной ситуации. Математической основой модели являются обобщённая модель J. Musa и физический принцип Н. М. Седякина. Они позволяют определять величину потребного вероятностного ресурса восстановления системы в работе и продолжительность предварительной тренировки операторов.**

Ключевые слова: **эргатическая система, оператор управления, нештатная ситуация, обучение, ликвидация, модель J. Musa, принцип Н. М. Седякина, ресурс восстановления.**

Введение

Современные сложные системы управляются, организуются, контролируются, обслуживаются и т. д. человеком или группой людей – операторов. Правильно осуществляемое между ТС и ЧС взаимодействие определяет максимально достижимый эффект. Этот эффект может быть экономическим, политическим. Во многих случаях от него может зависеть живучесть систем, жизнь, благосостояние групп или коллективов людей. Как достичь максимального эффекта в условиях решения конкретной задачи, которых может быть множество? Это зависит от ряда факторов и целевых установок, которые могут ставиться при решении задач. В целом охватить данную проблематику затруднительно, поэтому мы поставим и попытаемся решить сначала довольно простую, даже элементарную, задачу.

Прежде всего, следует отметить некоторые наиболее важные компоненты частей данных систем. В частности, что понимать под состоянием элементов и целых систем, от каких факторов и компонентов они зависят и т. д. Это проще всего рассматривать в пространстве-среде конкретной системы. Следует заранее указать множество трудностей, которые могут встретиться при построении количественных моделей систем.

При этом приходятся решать множество вопросов. Так, в статье [1] предложена классификация критериев оценки и пересмотра методов системного инжиниринга, которые применяются при анализе аварий в человеко-машинных системах. В [2] для анализа надежности человеко-машинной системы предлагается модель в виде непрерывной цепи Маркова, которая учитывает концепцию человеческих ошибок и факторов восстановления системы. Модель можно применять для общих систем, которые включают человеко-машинное взаимодействие.

Цели данной статьи – предложить простейшую математическую модель для оценивания отрицательного влияния человеческого фактора при управлении технической системой и дать рекомендации по его уменьшению.

Элементарная модель

Область программного прогноза

Создаётся сложная техническая система для выполнения предусмотренного задания в течение требуемого времени. Априорно оценивается и обеспечивается величина заданного показателя качества в течение этого времени работы системы. Допускается возможность возникновения наиболее вероятной нештатной ситуации в процессе её работы. Предполагается, что в случае её возникновения управляющий системой человек (звено) в течение некоторого времени сможет устранить неисправность в системе, и она продолжит работу. Для этой цели человек до начала применения системы по назначению должен быть заранее обучен устранять нештатную ситуацию. Спрашивается, сколько времени надо предусмотреть для устранения возможной нештатной ситуации.

Для решения этой задачи воспользуемся математической моделью J. Musa [3], предложенной им при оценивании надёжности программного обеспечения, которое до использования по назначению тестировалось для определения и устранения ошибок.

При условии, что в работе справедлив экспоненциальный закон безотказности, т. е. приработка и старение программного обеспечения исключены, действует следующее выражение для определения вероятности безотказной работы программного обеспечения:

$$P(t,\tau) = e^{-\frac{t}{T_0} e^{-\frac{\tau}{E_0 T_0}}}, \qquad (1)$$

где t, τ – время непрерывной работы по назначению и тестирования программы; T_0 – среднее время безотказной работы при $\tau = 0$; E_0 – начальное число ошибок в программе.

При произвольном распределении времени t, τ можно записать [4]:

$$P(t,\tau) = e^{-\int_0^t \lambda(z)dz \, e^{-\int_0^\tau \nu(\theta)d\theta}}, \qquad (2)$$

где $\lambda(t)$ – интенсивность отказов; $\nu(\tau)$ – интенсивность тестирования программы.

Пользуясь определением ресурса надёжности Н. М. Сидякина [5], представим (2) в виде

$$P(r(t), b(\tau)) = e^{-r(t)}e^{-b(\tau)}. \quad (3)$$

В дальнейшем условно будем называть $r(t)$ ресурсом расхода надёжности системы, $b(t)$ – ресурсом восстановления работоспособности системы.

В рамках поставленного вопроса – сколько времени надо предусмотреть для устранения возможной нештатной ситуации – сначала решим вспомогательный пример. Цель примера – показать, как связаны графически оба введённых ресурса.

Пример 1. Пусть вероятность выполнения задания системой задана в виде

$$P(r,b) = e^{-re^{-b}}, \quad (4)$$

где r, b – ресурсы расхода и восполнения работоспособности системы, соответственно. Представим их и вероятность в дискретном виде:

$$r_i = 1,2\ldots5;\ b_j = 1,2\ldots5;\ P_{i,j} = e^{-r_i e^{-b_j}}. \quad (5)$$

На рис. 1, 2 представлены графическая и матричная зависимости вероятностей. На рис. 1 даны кривые вероятностей с увеличением значений r_i на диагонали от левого верхнего угла к правому нижнему углу. Построена кривая вероятностей в зависимости от номеров i в порядке их возрастания от 1 до 5. Представим подробнее построение этой кривой на основе алгоритма линейной интерполяции [6]:

$$A(t) = linterp(x, y, t). \quad (6)$$

Для условий нашего примера запишем транспонированные координаты переменных по осям r, P:

$$r(1, 2, 3, 4, 5)^T;$$
$$P(0,692;\ 0,763;\ 0,861;\ 0,929;\ 0,967)^T. \quad (7)$$

Зависимость (7) представлена на рис. 3.

Из рис. 3 следует, что независимо от того, что величина ресурса r надёжности увеличивается (смещение в низ таблицы), значения вероятностей P на указанной диагонали возрастают.

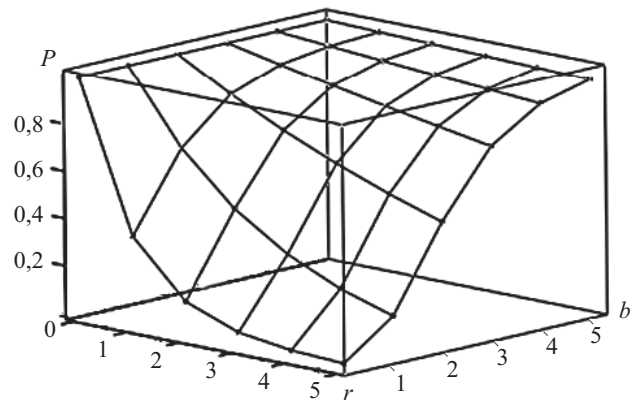


Рис. 1. Зависимость вероятности (4) от ресурсов r и b

$$P := \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.692 & 0.873 & 0.951 & 0.982 & 0.993 \\ 0 & 0.479 & 0.763 & 0.905 & 0.964 & 0.987 \\ 0 & 0.332 & 0.666 & 0.861 & 0.947 & 0.98 \\ 0 & 0.23 & 0.582 & 0.819 & 0.929 & 0.973 \\ 0 & 0.159 & 0.508 & 0.78 & 0.912 & 0.967 \end{pmatrix}$$

Рис. 2. Матрица вероятностей

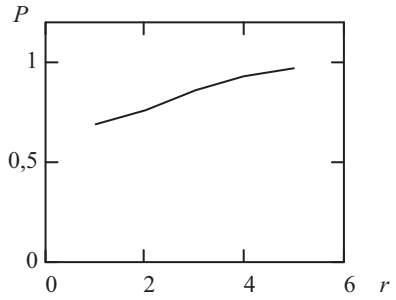


Рис. 3. Зависимость (7)

Это возрастание обусловлено тем, что с увеличением размера ресурса восстановления b значение экспоненты в показателе вероятности уменьшается, а сама вероятность P возрастает и при $b \to \infty$ будет стремиться к единице. Следует иметь в виду, что восстановление должно производиться до применения системы по назначению.

Теперь предположим, что система начинает подвергаться испытаниям до начала использования. Проводится ряд испытаний, чтобы выявить и устранить неисправности, которые в будущем могут нарушать процесс её штатной эксплуатации.

При этом предварительные испытания должны проводиться до тех пор, пока не появится возможность построить с достаточной точностью закон распределения восстановления после возникающих неисправностей. Благодаря этому человек приобретёт прочные навыки оперативного устранения нештатных ситуаций в процессе эксплуатации системы.

Поясним ещё раз, но более детально смысл формулы J. Musa, представленной в виде формулы (4). Обратите внимание, что оба ресурса в этой формуле вводятся одинаково и ступенчато. Цифры вероятностей первой колонки матрицы на рис. 2 по мере увеличения ресурса r (расхода надёжности) при единичном значении ресурса $b = 1$ (ресурса восстановления) монотонно уменьшаются от 0,692 до 0,159. Если $b = 2$ для второй колонки матрицы, то падение вероятностей будет менее значительным, а именно от 0,873 до 0,508. Если ввести ещё одну единицу ресурса, т. е. $b = 3$, то уменьшение вероятности станет ещё менее значительным: от 0,951 до 0,780. Наконец, для граничного значения столбца 5, где $b = 5$, уменьшение вероятности становится самым низким: от 0,993 до 0,967. Это показывает, насколько велико значение раннего (до эксплуатации) восстановления системы. На этом закончим изложение примера.

На рис. 4 дополнительно показано абсолютное постолбцовое уменьшение вероятности действия системы при заданных значениях $r, b = 5$:

$$b = (1,\ 2,\ 3,\ 4,\ 5)^T,$$

$$\Delta P = (0{,}533;\ 0{,}365;\ 0{,}171;\ 0{,}070;\ 0{,}026)^T.$$

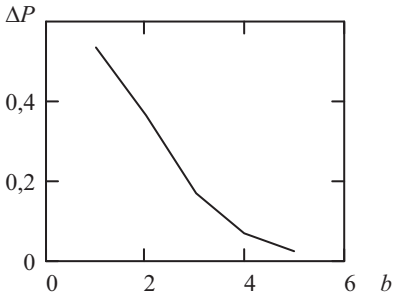


Рис. 4. Вероятность действия системы

Итак, на абстрактном конкретном числовом примере мы детально рассмотрели поведение вероятности функционирования системы, описываемой математической моделью J. Musa. Однако мы сознательно изменили предложенную им область приложения к оцениванию надёжности программного обеспечения с учётом его предварительного тестирования и исправления обнаруженных ошибок. Мы гипотетически заменили область приложения другой областью, предполагая до начала работы системы, что в ней возникнет нештатная ситуация, которая может изменить траекторию движения, но эта ситуация будет исправлена звеном управления, а система снова войдёт в нормальный режим.

Функционирование системы с одной нештатной ситуацией

До начала применения системы предполагается выполненным безошибочное априорное оценивание её работы в течение времени t:

$$P(t) = e^{-\int_0^t \lambda(z)dz}, \qquad (8)$$

т. е. величина ресурса

$$r(t) = \int_0^t \lambda(z)dz$$

известна, но на интервале $[0,t]$ может случайно возникнуть нештатная ситуация, которая может в дальнейшем нарушить нормальное поведение системы. Предположим, что закон распределения времени возникновения этой ситуации известен. Зададим его:

$$H(y) = 1 - e^{-\int_0^y \nu(z)dz}; \quad 0 \le y \le t. \qquad (9)$$

Допустимое время выхода из нештатной ситуации определяется законом

$$B(\theta) = 1 - e^{-\int_0^\theta \mu(z)dz}; 0 \le \theta \le d. \qquad (10)$$

Этот закон распределения должен быть установлен в результате предварительного обучения устранению нештатной ситуации управляющим звеном до применения системы.

В простейшем случае предположим, что закон (10) не зависит от времени возникновения ситуации в работе системы при эксплуатации. Тогда ресурс устранения ситуации будет

$$b(\theta) = \int_0^\theta \mu(z)dz, \qquad (11)$$

а вероятность выполнения задания системой –

$$P(r(t,b(d)) \approx e^{-r(t+d)e^{-b(d)}}. \qquad (12)$$

В общем случае, когда нештатная ситуация происходит в момент времени y и продолжительность её устранения связана с этим моментом,

$$b(\theta, y) \approx \int_0^{\theta(y)} \mu(y)dy,\ 0 \le \theta(y) \le d(y), \qquad (13)$$

соответственно, вероятность выполнения задания системой станет более сложной:

$$P(r(t,b(d(y))) \approx e^{-r(t+d(y))e^{-b(d(y))}}. \qquad (14)$$

Знак ≈ применён для того, чтобы при записи избежать использования операции интегрирования.

Если в процессе функционирования системы предусматривается более одной нештатной ситуации, то алгоритм вычисления вероятности значительно усложнится. В отдельных случаях, на наш взгляд, для решения задачи может применяться имитационное моделирование.

Численная реализация этого алгоритма, даже сравнительно несложного по структуре, потребует приложения значительных усилий, поэтому для иллюстрации вероятностных расчётов рассмотрим прикладной пример с применением другого алгоритма.

Пример 2. Безотказность управляемой технической системы характеризуется следующими численными параметрами: время непрерывной работы $10h.$; априорно определённое распределение времени до отказа задано нормальной плотностью вероятности $f(t) = dnorm(m,\sigma,t)$, $m = 100\,h.$, $\sigma = 12\,h.$, поэтому вероятность её безотказной работы составляет $P(10) = 0{,}993$. На ней может возникнуть одна нештатная программная ситуация, приводящая к нарушению работоспособности системы.

Распределение нарушения происходит по экспоненциальному закону с интенсивностью $\lambda = 0{,}2h^{-1}$, средняя величина ресурса надёжности $r = 2\,h$, значение первой экспоненты в формуле J. Musa будет $e^{-2} = 0{,}135$. Чтобы сохранить работоспособность технической системы на уровне $P(10) = 0{,}993$ после устранения нештатной ситуации, потребуется значение ресурса восстановления $b = 9{,}903$ с вероятностью 0,9999, которая подбирается опытно для **постановки** и получения в результате решения уравнения

$$e^{-2e^{-b}} - 0{,}9999 = 0.$$

Спрашивается, сколько испытаний надо предварительно провести, чтобы подтвердить эту вероятность, и какое время

затратить, если на один прогон программы требуется $\tau = 0,005\,h$. Итак, вероятность отсутствия ошибки $p = 0,9999$, а вероятность ошибки $q = 0,0001$. Среднее число ошибок в n испытаниях равно np, среднеквадратическое отклонение $\sqrt{npq}$, поэтому плотность вероятности числа испытаний представим в виде

$$g(x) = \frac{C}{\sqrt{2\pi npq}} e^{-\frac{(x-np)^2}{2npq}}; \quad C = 1,852.$$

Данная плотность превращается в дельта-функцию при $n = 100$, поэтому время испытаний становится равным $n\tau$. Если за время функционирования системы $10\,h$. произойдёт одна нештатная ситуация, то время испытаний составит $0,5\,h$. Вероятность выполнения задания системой сохранится прежней, т. е. $P = P(10)\,e^{-2e^{-b}} = 0,993$. Если же в системе ожидается 10 нештатных ситуаций, тогда вероятность выполнения задания системой становится $P = P(10)e^{-2e^{-0,99}} = 0,472$. Это означает, что предварительных испытаний программного обеспечения по устранению нештатных испытаний было недостаточно, так как вероятность исправной работы системы меньше расчётной $P < 0,993$.

Дискретное представление ресурса

В теории надёжности рассматривается непрерывное представление ресурса

$$r(t) = \int_0^t \lambda(z)dz = -\ln P(t).$$

Ресурс понимается в смысле профессора Н. М. Седякина. При испытаниях программного обеспечения приходится использовать не непрерывное время, а время, представляемое в дискретном виде, а именно в количестве прогонов программы, поэтому имеет смысл выражать ресурс в зависимости от числа прогонов программы. Предложим модель ресурса, зависящего от числа прогонов. Сначала запишем выражение для вероятности безотказной работы для непрерывного времени испытаний:

$$P(t) = \frac{N_0 - n(t)}{N_0}, \qquad (15)$$

где N_0 – количество объектов, первоначально поставленных на испытание, $n(t)$ – количество объектов, отказавших за время испытаний t.

Представим, что время t представлено дискретно $t = m\tau$, где τ – время одного кванта (дискрета), а m – полное число квантов за время до отказа. Первоначальное число объектов представим в виде n_0. Тогда

$$P(n_0\tau) = \frac{n_0\tau - m\tau}{n_0\tau} = 1 - \frac{m}{n_0}. \qquad (16)$$

Далее предположим, что формула (16) верна лишь для некоторого времени t_i, $i = 1, 2, \ldots, \; t_{i+1} > t_i$ для всех i, поэтому (16) можно представить в виде $P(t_i) = 1 - \frac{m_i}{n_i}(t_i)$, а величину дискретного ресурса –

$$r_i(t_i) = -\ln[1 - \frac{m_i}{n_i}(t_i)]. \qquad (17)$$

Это касается только ресурсов для формулы J. Musa ($r_i(t_i)$, $b_i(t_i)$ программного обеспечения), но не относится к ресурсу аппаратуры с непрерывным временем её функционирования. Расчёт безошибочности работы системы выполняется так же, как указано выше.

О требованиях к технической системе и человеческому звену управления

Если к системе предъявляются особые требования: не только вероятность выполнения ею задания, но и, например, безопасность экипажа, величина ущерба и риска и другие, то необходимо учитывать ряд дополнительных системных параметров. С учётом значений этих параметров необходимо скорректировать предлагаемую модель с целью выполнения экстремальных решений известными методами для получения желаемого результата.

Заключение

В статье предложена модель для снижения влияния нештатных ситуаций при функционировании сложной системы. Эти нештатные ситуации ликвидируются силами человеческого управляющего звена. Для увеличения эффекта ликвидации звено управления должно предварительно (до применения системы) по назначению обучаться в лабораторных условиях. При этом имитируется необходимый мониторинг исходных данных для ликвидации нештатной ситуации в работе системы.

В качестве математической модели предложено использовать модель J. Musa, применяемую при тестировании программного обеспечения. Дан алгоритм для определения необходимого ресурса восстановления в нештатной ситуации. Характеристики алгоритма служат руководством при ликвидации нештатной ситуации. Приведены элементарные примеры численных расчётов для данной эвристической модели. Сформулированы рекомендации для практической реализации предлагаемой модели.

Однако модель нецелесообразно применять к комплексу «техника и программное обеспечение», так как математическая модель J. Musa не предназначена для доработок по устранению отказов и неисправностей, тем более – в совокупности с ошибками программного обеспечения.

Для примера укажем ряд современных работ, в которых затрагиваются близкие вопросы моделирования человеко-машинных систем. В частности, в [7] рассматриваются особенности формирования информационной модели в информационной системе и ее взаимодействие в человеко-машинной технологии обработки информации. В [8] предлагается решение задачи построения рационального плана наблюдений параметров состояния человеко-машинных систем на основе контроля. В [9, 10] рассматриваются вопросы моделирования геодезических систем – маркшейдерских эргатических систем (Mine Surveying Ergatic System – MSES). Поисково-разведочные работы выполняет группа людей, включая маркшейдера (специалиста) и одного или двух шахтеров. Учитываются особенности функционирования системы, ее составляющие (человек – маркшейдер, оборудование – геодезический инструмент, минирование, окружающая среда).

Литература

1. Liu C. M. Reliability model of a man-machine system with human errors and its applications / C. M. Liu, A. H. Wang // J. Chin. Inst. Eng. – 1998. – № 21 (2). – P. 149–158.

2. Kontogiannisa T. A comparison of accident analysis techniques for safety-critical man–machine systems / T. Kontogiannisa, V. Leopoulosb, N. Marmarasb // Int. J. Industrial Ergonomics. – 2000. – Vol. 25, Is. 4. – May. – P. 327–347.

3. Musa J. A theory of software reliability and its application / J. Musa // IEEE Trans. on software Eng. – 1975. – Vol. SE-1, Sept. – P. 312–327.

4. Смагин В. А. Дискретный аналог математической модели J. Musa и рекомендации по его применению в исследовании безошибочной работы коллективов и надёжности программного обеспечения / В. А. Смагин // Тр. ВКА им. А. Ф. Можайского. – 2007. – Вып. 621. Современное состояние и перспективы развития технологии автоматизированного управления и связи. – 163 с.

5. Седякин Н. М. Об одном физическом принципе теории надёжности / Н. М. Седякин // Изв. АН СССР. Технич. кибернетика. – 1966. – № 3. – С. 80–87.

6. Кирьянов Д. В. MathCAD 12 / Д. В. Кирьянов. – СПб.: БХВ-Петербург, 2005. – 576 с.

7. Матчин В. Т. Информационная модель в человеко-машинной системе / В. Т. Матчин // ПНиО. – 2014. – № 6 (12). – URL : http://cyberleninka.ru/article/n/informatsionnaya-model-v-cheloveko-mashinnoy-sisteme (дата обращения 29.03.2017).

8. Розенбаум А. Н. Планирование наблюдений в человеко-машинной системе / А. Н. Розенбаум, А. И. Никитин // Вестн. АГТУ. Сер. Морская техника и технология. – 2011. – № 2. – URL: http://cyberleninka.ru/article/n/planirovanie-nablyudeniy-v-cheloveko-mashinnoy-sisteme (дата обращения 29.03.2017).

9. Zverevich V. V. Theoretical and Experimental Study of Mine Surveyors Testing / V. V. Zverevich, V. M. Tsaplev, G. P. Zhukov, A. L. Ivanova // Open Access Library J. – 2016. – 3: e3020. – URL: http://dx.doi.org/10.4236/oalib.1103020.

10. Zverevich V. V. A Mathematical Model of Mine Surveying WorkTime / V. V. Zverevich, V. M. Tsaplev // Am. J. Envir. Eng. Sci. – 2015. – № 2. – P. 60–64.

Heuristic Model of Liquidation of Supernumerary Situations in Man-Machine Control Systems

Smagin V.A.
A.F. Mozhaysky Military Space Academy,
St. Petersburg, Russia
va_smagin@mail.ru

Abstract. **The model for liquidation of the supernumerary situation arising in work of man-machine system is offered. The model consists of two parts: a stage of preliminary training and training of operators of management in vitro before work of system and a stage of direct liquidation by operators of a supernumerary situation in its work. A mathematical basis of model is generalized model J. Musa and N.M. Sedjakin's physical principle. They allow define size required a likelihood resource of restoration of system in work and duration of preliminary training of operators.**

Keywords: **man-machine system, the operator of management, a supernumerary situation, training, liquidation, model J. Musa, N.M. Sedjakina's principle, a restoration resource.**

References

1. Liu C.M., Wang A.H. Reliability model of a man-machine system with human errors and its applications,*J. Chin. Inst. Eng*., 1998, no. 21 (2), pp. 149-158.

2. Kontogiannisa T., Leopoulosb V., Marmarasb N. A comparison of accident analysis techniques for safety-critical man–machine systems, *Int. J. Industrial Ergonomics*, 2000, Vol. 25, Is. 4, May, pp. 327-347.

3. Musa J. A theory of software reliability and its application, *IEEE Trans. on software Eng*., 1975, vol. SE-1, Sept., pp. 312-327.

4. Smagin V.A. A discrete analog of the mathematical model of J. Musa and recommendations for its application in the study of error-free work of teams and reliability of software [Diskretnyi analog matematicheskoi modeli J. Musa i rekomendatsii po ego primeneniiu v issledovanii bezoshibochnoi raboty kollektivov i nadezhnosti programmnogo obespecheniia], *Trudy VKA imeni A.F. Mozhaiskogo [Proc. ACA named A. F. Mozhaisky]*, 2007, Is. 621, 163 p.

5. Sediakin N.M. On a physical principle of the theory of reliability [Ob odnom fizicheskom printsipe teorii nadezhnosti], *Izv. AN SSSR. Tekhnicheskaia kibernetika [Izv. Acad. Sci. USSR. Technical Cybernetics]*, 1966, no 3, pp. 80-87.

6. Kiryanov D.V. MathCAD 12. St. Petersburg, BHV-Petersburg, 2005, 576 p.

7. Matchin V.T. The information model in man-machine system [Informatsionnaia model' v cheloveko-mashinnoi sisteme], *Psihologicheskaya nauka i obrazovanie [Psychological Science and Education]*, 2014, no. 6 (12). Available at: http://cyberleninka.ru/article/n/informatsionnaya-model-v-cheloveko-mashinnoy-sisteme (accessed 29.03.2017).

8. Rozenbaum A.N., Nikitin A.I. Planning of observations in the man-machine system [Planirovanie nabliudenii v cheloveko-mashinnoisisteme], *Vestnik AGTU. Seriia: Morskaia tekhnika i tekhnologiia [Bull. ASTU. Series: Marine technology and technology]*, 2011, no 2. Available at: http://cyberleninka.ru/article/n/planirovanie-nablyudeniy-v-cheloveko-mashinnoy-sisteme (accessed 29.03.2017).

9. Zverevich V.V., Tsaplev V.M., Zhukov G.P., Ivanova A.L. Theoretical and Experimental Study of Mine Surveyors Testing, *Open Access Library J.*, 2016, 3: e3020. http://dx.doi.org/10.4236/oalib.1103020.

10. Zverevich V.V., Tsaplev V.M. A Mathematical Model of Mine Surveying WorkTime, *Am. J. Envir. Eng. Sci.,* 2015, no 2, pp. 60-64.

Homogeneity Principle for Cryptographic Protocol Analysis and Synthesis

Aleksandrova E. B.
Peter the Great St. Petersburg Polytechnic University
St. Petersburg, Russia
helen@ibks.spbstu.ru

Abstract. **Homogeneity principle for analysis and synthesis of cryptographic protocols is introduced, due to which increasing the number of mathematical problems does not increase the security of underlying information system. The comparison of two authentication protocols in accordance with this principle is given. The ways to reduce complexity heterogeneity in digital signature protocol are proposed.**

Keywords: **cryptographic protocol, digital signature, elliptic curve discrete logarithm problem, complexity, homogeneity.**

Introduction

Security of cryptographic algorithms and protocols is based on mathematical problems. They can be unaltered and variable. These problems come from different cryptographic primitives. As a rule, to break cryptosystem security it is sufficient to solve any of these mathematical problems. The complexity of these problems decreases in time, so it seems natural to subdue all of them to the basic problem, i. e. the problem with the highest complexity.

The complexity homogeneity principle is considered, and some ways of its use for analysis and synthesis of cryptographic protocols are proposed.

Hierarchy of mathematical problems

The security of large cryptographic systems is based on diverse cryptographic primitives: symmetric and public key encryption, digital signature, zero knowledge proof, etc. Security of cryptographic primitives is based on the complexity of mathematical problems. The number of such problems is tens and even hundreds:

• the problem of key breaking and keyless reading for different ciphers [1];

• integer factorization problem, to which RSA problem can be reduced [2];

• square root problem, to which Rabin [3] and Fiat–Shamir [4] cryptosystem problems can be reduced;

• discrete logarithm problem in a multiplicative group of prime field, to which Elgamal [5] problem can be reduced;

• discrete logarithm problem in a multiplicative group of extended field, to which Diffie – Hellmann [6] problem can be reduced;

• elliptic curve discrete logarithm problem, to which GOST R 34.10-2012 [7] problem can be reduced;

• the problems of ideal classes group of on number fields [8];

• the subset sum and knapsack problem [9];

• the problem of elliptic curve isogeny computation [10–13];

• lattice-based problems [14–16], etc.

It is important to classify these problems, reflecting both the peculiarities of the problems and methods of their solution. It seems natural to divide these problems into the following unified classes [1]:

• security of ciphers for known plaintexts is based on Boolean satisfiability problem. Under the assumption that plaintexts and corresponding ciphertexts define the key uniquely (to achieve this, the known plaintext is to be 1,38 times longer than the key). If encryption operations are presented in the form of Booolean functions, substituted each other, then every bit of intermediate text is computable Boolean function of the key. Let objective function be conjunction of bitwise equalities of the values of Boolean functions, corresponding to ciphertext, and the values of true ciphertext. This function is computable and holds true for the true key only;

• integer factorization problem for $n = pq$ in RSA cryptosystem can be reduced to the problem of order and structure computation in finite Abelian group. Indeed, if the order $\phi(n) = (p-1)(q-1)$ of the group $\mathbf{Z}_n^*$ is known, the divisors of n are the roots of polynomial $x^2 - (n - \phi(n) + 1)x + n$;

• discrete logarithm problems in different cyclic groups represent the unified discrete logarithm problem in the cyclic group of computable order;

• the knapsack cryptosystems problems can be reduced to the unified knapsack problem;

• the problem of elliptic curve isogeny computation is a special case of the problem of computing the morphism in Abelian groups category.

Parameterization of these classes of unified problems with mathematical structures (ciphers, groups, categories) gives a basic mathematical problem. Thus, the methods of unified problems solution are obviously applicable for basic problems.

The more complex is the problem, the more secure is corresponding cryptographic algorithm or protocol. But the complexity decreases in time with the rate $s(t,T) = \dfrac{\log S(T) - \log S(T+t)}{t \log S(T)}$, where $S(T)$ is the strength in the initial time T [1]. This formula can be interpreted as the decrease of the initial brute force cryptographic algorithm strength per one bit of the key. The expression for $s(t, T)$ can be written as $\log S(T+t) = (1 - ts(t, T))\log S(T)$, from which $S(T+t) = S(T)^{1-ts(t,T)} = e^{(1-ts(t,T))\ln S(T)}$. So if $s(t, T)$ changes slightly, the dependence $S(T+t)$ for the symmetric iterated cipher or a hash function can be approximately described by a falling exponent.

However, the rate of complexity falling is different for different mathematical problems and cryptographic algorithms. For example, the complexity of key breaking for symmetric ciphers falls by about a constant speed, equal to 0,023 year^{-1}. At the same time, the complexity of factorization problem falls unevenly and depends on the length of composite number [1].

So, the problem complexity depends not only on its size but on time also. When constructing cryptosystems it is necessary to predict the high complexity of mathematical problems at least for a few years. If at the time of project completion the problem A is more difficult than the problem B of the same (or different) size, it does not mean that the same ratio will continue in ten years.

For analysis of mathematical problems the relation of polynomial reducibility is used often, which does not depend on the current complexity estimation. The problem A is not more difficult than the problem B, if we can solve every partial problem A by deterministic polynomial algorithm, knowing the solution of the problem B. We can say also that the problem A can be reduced to the problem B. If the reverse reduction holds also, the problems A and B are called equivalent.

Polynomial reduction allows allocating in the set S of mass mathematical problems a subset of problems to which given mass problem A can be reduced. Let call the subset S_A of those problems, to which the problem A can be reduced, the problems, associated with A. For example, elliptic curve discrete logarithm problem over prime finite field $\mathbf{F}_p$ can be reduced to one of the following problems:

• discrete logarithm problem in multiplicative group of finite extension of the field $\mathbf{F}_p$, resulting from Weil pairing [17];

• the problem of Mordell–Weil group computation of the curve $E(K)$, given over the number field $K = \mathbf{Q}[\alpha]$, where the root of minimal polynomial for α is in $\mathbf{F}_p$, and the problem of point lifting from finite field to the number one [18].

As usual, cryptographic algorithm or protocol security depends not on one but on several problems, solving any of which violates its security. If none of these problems is associated with the others, we call these problems heterogeneous.

Homogeneity principle

Cryptosystems are often made heterogeneous, with different algorithms of encryption, hashing, digital signing, etc. It may seem that it is easier for intruder to solve one problem instead of several. But in practice it is sufficient to solve one problem, which is the easiest at this point of time.

For example, if in cryptographic system the session key of the symmetric cipher is established by the Diffie – Hellman protocol and digital signature is used, then it is enough to solve any of the problems: compute the symmetric cipher key, break Diffie – Hellman or break signature key, to violate security. In the latter case, the intruder can impersonate a legitimate user towards another user or to implement a man-in-the-middle attack.

Let $A_1, \ldots, A_l$ form the set of problems, on the complexity of which cryptographic algorithm security is based. The relation of polynomial reduction divides this set into equivalence classes of associated problems. Then the problems, belonging to different classes, will be heterogeneous.

We call the number of heterogeneous problems, forming the base of cryptosystem security, homogeneity of complexity. The following proposition holds.

Proposition 1. Let cryptographic algorithms C_1 and C_2 are such that in order to violate algorithm C_1 security we are to solve problem A, and to violate algorithm C_2 security we are to solve one of heterogeneous problems A or B. Then algorithm C_2 is not more secure than algorithm C_1.

Proof. Let S_A, S_B be the complexities of the problems A and B correspondingly. According to the absorption law, $S_A \geq \min(S_A, S_B)$.

Corollary. Increasing the number of different heterogeneous problems in cryptographic algorithm does not increase its security.

Now we can formulate *complexity homogeneity principle*: we need to decrease the number of heterogeneous problems while cryptosystem construction [19]. Thus, conglomeration of heterogenious ciphers, random number generators, hash functions, signatures, and other authentication algorithms in a large information system are useless and even potentially dangerous.

Cryptographic protocols analysis and synthesis

In practice, cryptographic protection is implemented in the form of cryptographic protocols. Indeed, it is not enough only to encrypt data, you must generate encryption keys and deliver them to users, change the keys in time, and provide authentication. This raises a set of different applied problems, which are solved with the help of certain cryptographic protocols. The security of a whole system is determined by the composition of all cryptographic protocols.

The problem of protocol analysis and synthesis is one of the main problems in cryptography. A complete solution of this problem requires a large amount of research on analysis of all basic and associated mathematical problems, the analysis of the security of actual protocols and security analysis of complex protocols in view of their interdependence. In this case, since the complexity of mathematical problems change over time, the result of the research will reflect the real situation only at the time of the end (or even beginning) of these studies. So, let's consider a simplified approach to analysis and synthesis of protocols due to homogeneity principle.

If there are two cryptographic protocols, the first is based on the problems set A; and to break security it is sufficient to solve any of them; the second is based on the problems set B, where $A \supseteq B$, then the first protocol is not more secure than the second one.

The specified ordering of protocols allows comparing their security, and to optimize the composition of protocols, including the issues of key and auxiliary random numbers generation. The question of analysis and optimization is to formalize a set of problems underlying the security, and to minimize this set.

This set consists of base and variable problems. For example, in digital signature standard GOST R 34.10-2012 [7] elliptic curve discrete logarithm problem cannot be change. At the same time, algorithms for generating auxiliary and a secret key are not regulated by any procedure, that is, the related problems can vary. Among the varied algorithms there exists optimal for which a problem of security breach is not easier than elliptic curve discrete logarithm problem.

Comparative analysis of authentication protocols

Consider two identical elliptic curve protocols of multiple authentication based on digital signature and public-key encryption. The first party proves its authenticity, and the second checks it. It is believed that prover does not trust verifier.

In the first protocol, verifier generates a random request and sends it to the prover, who signs it according to GOST R 34.10-2012. Prover generates signature and sends it to the verifier. The latter checks the validity of the signature.

In the second protocol, verifier generates a random request, encrypts it with public key and sends to the prover for decryption. Prover decrypts the message using secret key and sends it to the verifier who compares this text with the original.

These two protocols are solving the same problem: the verifier makes sure that the prover knows the secret key (signature key or decryption key). Both protocols are implemented on the same elliptic curve. Which of them is safer? Analysis due to homogeneity principle allows answering this question.

Let's consider digital signature protocol from GOST R 34.10-2012 [7].

Let $E(\mathbf{F}_p)$: $y^2 = f(x)$ be elliptic curve with j-invariant not equal to 0 and 1728, m be the message to be signed, h be hash-function, $P \in E(\mathbf{F}_p)$ be generator of order r. So $\{E(\mathbf{F}_p), P, Q\}$ is public key, integer d, where $Q = dP$ is private key. To sign the message m, the sender computes $e \equiv h(m) \pmod r$, and if $e = 0$ sets $e = 1$; generates integer k, $0 < k < r$, at random and computes $R = (x_R, y_R) = kP$, where $x_R \neq 0 \pmod r$; computes $s \equiv (dx_R + ke) \pmod r$, where $s \neq 0$.

The signature verification needs the following: check that $0 < x_R \pmod r < r$ and $0 < s < r$; compute $e \equiv h(m) \pmod r$ and if $e = 0$ set $e = 1$; compute $R' = (se^{-1} \pmod r)P - - (x_R e^{-1} \pmod r)Q$. If $x_{R'} \equiv x_R \pmod r$ holds then the signature is valid.

The security of digital signature protocol directly depends on the complexity of hash function inversion and the difficulty of computing collisions of a hash function, as in the first case it is possible to calculate the message for an existing signature, and in the second to prepare a couple of messages with the same value e to sign one of them, and then replace one message by another. The complexity of computing hash function collisions by Pollard's algorithm is equal to $S = O(\sqrt{r})$.

This protocol involves stringent requirements for the random number generator: If the random number k is predictable (computable) at least once or repeats during the public key lifetime, the signature key can be computed with polynomial complexity.

Note that to break secret signature key it is sufficient not only to predict a random number, which will appear in future, but to find a random number that was previously used. For example, if the intruder has gained access to an algorithmic random number generator, allowing recovery of earlier state from the current, all digital signatures created on this current key should be considered invalid. Therefore, if the potential unauthorized access (for example, when sending a computer for repair due to the failure) to computer, that implements the signature generation is possible, and if the random number generator is implemented algorithmically, the algorithm of random number generation must be irreversible.

For secret key d computation it is sufficient to solve one of discrete logarithm problems: for the points P and Q or for the points P and R (the value x_R is easily restored from its residue $x_R \pmod r$, and the coordinate y_R can be computed as $\sqrt{f(x_R)} \pmod p$). Thus, the requirements for the random number generator, are more rigid than for the key one: the intruder is still what to look for: k or d, but d can be computed from k. Thus, Kolmogorov entropy of digital signature key does not exceed the entropy of the random numbers from generator [1].

So the security of GOST R 34.10-2012 is based on the following heterogeneous assumptions.

1. Elliptic curve discrete logarithm problem is hard (the solution of this problem leads to the disclosure of secret key).

2. Kolmogorov entropy of random bit generator is not less than Kolmogorov entropy of key generator (otherwise, the signature strength will be reduced in compare to the design rating).

3. Probability of two equal random numbers during the key life period is negligible (otherwise, one can expect to the disclosure of secret key with a low complexity).

4. Hash-function h is computationally irreversible (otherwise, one can substitute the signed message to the other).

5. Hash-function collision computation problem is hard (otherwise, one can prepare a couple of messages that make up collision, and to replace the signed message to the other after signing).

Now let's consider public key encryption protocol [1], based on Diffie – Hellmann and Elgamal protocols. The common parameters are elliptic curve $E(\mathbf{F}_p)$ and the point $P \in E(\mathbf{F}_p)$ of order r. Point $Q \in \langle P \rangle$ is a private key, and integer d, such that $Q = dP$ is public key. Hash function h is used and plaintext m is from $0 \le m \le r - 1$.

Verifier chooses integer k at random, and computes $R \leftarrow kP$, $e \leftarrow h(kQ)$, $c \leftarrow (m + e) \pmod r$. Ciphertext is a tuple (R, c).

Pretender in the authentication protocol computes $e \leftarrow h(dR)$ and $m \equiv (c - e) \pmod r$.

The security of this protocol is based on Diffie–Hellmann problem: given points P, $Q = dP$, $R = kP$, compute $kdP = kQ = dR$. This problem is reduced in polynomial time to the elliptic curve discrete logarithm problem, as it is sufficient to compute one of logarithms k or d for its solution.

The requirements imposed on random bit generator here are less stringent than in signature protocol. The point R is not to be used more than once, because a single computation of a random number k allow decrypting a message m encrypted with this number, but not to compute the key (as in digital signature protocol). Similarly, the repetition of the random number k allows decrypting one of the messages if the other, encrypted with this k, is known.

Hash function and the arithmetic in $\mathbf{Z}_r$ are needed to eliminate practical redundancy, which presents in elliptic curve point coordinates. Such redundancy is due to the fact that the length of two coordinates equals to $2\log_2 p$, and the length of the group order is $\log_2 r$, where r is no longer than p.

The set of heterogeneous problems here consists of three ones, and is a subset of the set from digital signature protocol. Therefore, it can be argued that if the discrete logarithm problem and Diffie – Hellmann problem are equivalent, then public key encryption protocol is not less secure than digital signature one.

Both private and public keys of digital signature are to be changed periodically. Furthermore, hash-function initial vector is to be changed: if the collision is computed, there is a danger for all the cryptosystem users.

So, if the signer can generate random numbers, he also can generate his own private key. It follows from homogeneity principle that for GOST R 34.10-2012 algorithmic generator, equivalent to the elliptic curve discrete logarithm problem, is optimal. Such generator, with regard to the signature protocol, is not worse than the "ideal" strong random number generator.

Similarly, one can determine the optimal key generators for symmetric ciphers: keys are to be generated algorithmically with the same cipher. Thus, the principle of complexity homogeneity allows determining the best key generator for this cryptographic algorithm.

Strengthening the signature protocol

The first way to decrease the number of heterogeneous mathematical problems is to modify hash-function and to include auxiliary random elliptic curve point into its argument.

If we use $e' = h(m||x_R \pmod r) \pmod r$ instead of e in digital signature protocol, then protocol holds, but excludes the attack based on the prepared hash function collisions. The value e' can be computed not only by the signer but by verifier, so it is correct. Replacing e with e' does not reduce the cryptographic strength of the signature protocol, but eliminates the attack based on the prepared hash function collision. To prove this, it is sufficient to consider the impact of this substitution on the problem of the treatment and calculation of hash function collisions. To inverse the value e it is needed to find m, and to inverse e' it is needed to solve the same problem, provided that the remaining part of the argument is fixed and is equal to $x_R \pmod r$. Obviously, if one can inverse e, then he can inverse e' (it is sufficient a portion of the argument bits be fixed). The same considerations apply in terms of collisions computation for two variants of a hash function.

However, if in the original version of the protocol, the intruder may seek collisions only through initial vector life time, in the second case, he can do this only during the interval between the procedures of signature generation and verification. In the original version, the intruder may participate in initial vector generation and to combine his choice with the collisions search. In the second case, such an attack is impossible, since the values $x_R \pmod r$ are always different (the same values lead immediately to the key disclosure in both cases). Thus, replacing e with e' is a strict strengthening of the signature protocol.

In addition, iterative hash function with the fixed input size can be used instead of the hash function GOST R 34.11-2012. To construct it one can use one way function, which is collision-free for the arguments of $n \le ([\log_2 r] - 2)/2$ bits length, where r is the order of elliptic curve points group. In this case, elliptic curve discrete logarithm problem is reduced to the problem of hash function inversion. For this purpose, hash function from [20] can be adapted to elliptic curves.

If standard hash function h is needed (for example, GOST R 34.11-2012 [21]), one can use $e' = x_{h(m)P} \pmod r$. Here e' depends on $h(m)$, so it is natural to assume that to invert e', one must firstly compute $h(m)$ from $h(m)P$, i. e. to solve elliptic curve discrete logarithm problem. Elliptic curve is to be the same as in digital signature protocol.

The second way is to use algorithmic elliptic curve random bit generator, for which elliptic curve discrete logarithm problem is reduced to the problem of random number prediction and to the problem of previous generator state computation. Such generator can be given by the following recurrent equation. Let $T_i = (x_i, y_i)$ be the current point of the same elliptic curve $E(\mathbf{F}_p)$ as in digital signature protocol, and integer $r - p$ is at least as maximum length of generator period. The next state is given as $T_{i+1} = (i + x_{T_i})P$. The dependence of the point of the number of iteration i is to prevent "looping" after a small number of iterations, and cannot be considered a cryptographic enhancement. Generator returns some (for example, 16) less significant bits of x_{T_i}.

Generator state inversion problem is to compute the next state from the current one.

Proposition 2. The problems of elliptic curve discrete logarithm and generator state inversion are equivalent.

Proof. Every point T_{i+1} corresponds to unique logarithm $i + x_{T_i}$, so the only one previous state T_i is possible. So, every point $-T_{i+1}$ with the same x-coordinate corresponds to the unique previous state $-T_i$. So every generator state is defined up to elliptic curve automorphism (if j-invariant is not equal to 0 and 1728, then automorphism group consists of two elements ±1). The set of logarithms in generator equation is a subset of all possible elliptic curve discrete logarithms.

If elliptic curve discrete logarithm problem is solved, then one can compute the previous state T_i from the current state T_{i+1}, i. e. generator inversion problem is reduced to elliptic curve discrete logarithm problem.

If generator inversion problem is solved, then one can compute the previous state T_i from the current state T_{i+1}, for any initial logarithm corresponding to the point T_0. So it is possible to compute elliptic curve discrete logarithm of the form $i + x_{T_i}$. While changing logarithm of the initial point T_0, one can get the full set oa possible logarithms, coinciding with the set of remainders modulo r. So, Следовательно, elliptic curve discrete logarithm problem is reduced to generator inversion problem. ■

The prediction of the next state of the generator, when a part of random sequence is known, reduces to the calculation of x_{T_i} from one or several least significant bits of x-coordinate of T_i and previous points. Numerous experiments have shown that when 16 least significant bits are used, then bits, pairs, triples, …, eights of bits are statistically distributed at uniform.

According to [22], the problem of prediction of generator state, if some previous elements are known, can be reduced to the discrete logarithm problem.

This generator is not the only possible one. One can build a random number generator on elliptic curve based on a recursive hash function without collisions with the brute force complexity of inversion (see, [1]), for which the dependence of iteration number is not needed. Moreover, the following condition can be used instead of least significant bits of x-coordinate: if $y < p/2$ then generator outputs 0, otherwise generator outputs 1. The y-coordinate of the point of order r is not zero, and for every $T = (x, y)$ there exists $-T = (x, p - y)$, so such generator outputs 0 and 1 equiprobably.

Not only digital signature, but zero-knowledge proof can be used for multiple messages authentication in the conditions of the untrusted verifier. It can be shown that zero-knowledge proof protocol is of the same homogeneity as digital signature one, but it requires to transfer far greater amounts of proprietary information and is of less speed. So zero-knowledge proofs based on elliptic curve discrete logarithm problem have no advantages in comparison with digital signature.

Conclusion

The reduction of the number of mathematical problems, underlying the security of cryptographic algorithms and protocols, and the primitives conformation to the most hard problem is

gaining more and more widespread. In recent years, random number generators and hash functions had been proposed, whose security is based on a new, so-called post-quantum mathematical problems of the theory of lattices and isogenies of elliptic curves (see, for example [23–26]). Thus, the formulated complexity homogeneity principle can be used and expanded not only in existing practical purposes but also for future cryptographic systems.

References

1. Rostovtsev A. G., Makhovenko E. B. *Teoreticheskaya kriptografiya* [Theoretical Cryptography], St. Petersburg, Professional, 2005, 480 p.

2. Rivest R. L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, 1978, Vol. 21, no. 2, pp. 120-126.

3. Rabin M. Digitalized signatures and public key functions as intractable as factorization. – *MIT Laboratory for Comp. Sci. Technical Report MIT/LCS/TR–212*. 1979.

4. Fiat A., Shamir A. How to prove yourself: Practical solutions to identification and signature problems, *Cryptology – CRYPTO'85. LNCS*, 1990, Vol. 263, pp. 186-194.

5. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms/T. ElGamal, *IEEE Trans. Inf. Theory*, 1985, Vol. IT-31, pp. 469-472.

6. Diffie W., Hellman M. New directions in cryptography, *IEEE Trans. Inf. Theory*, 1976, Vol. IT-22, pp. 644-654.

7. *GOST R 34.10-2012 Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Protsessy formirovaniya i proverki elektronnoy tsifrovoy podpisi* [Information technology. Cryptographic data security. Signature and verification processes of [electronic] digital signature], Moscow, Standartinform, 2013, 29 p.

8. Buchmann J., Maurer M., Moller B. Cryptography based on number fields with large regulator, *J. Théorie des Nombres de Bordeaux*, 2000, Vol. 12, no. 2, pp. 293-307.

9. Chor B., Rivest R. A knapsack-type public key cryptosystem based on arithmetic in finite fields, *IEEE Trans. Inf. Theory*, 1988, Vol. IT-34, pp. 901-909.

10. Bröker R., Charles D., Lauter K. Evaluating large degree isogenies and applications to pairing based cryptography, *Pairing-Based Cryptography – Pairing 2008*, LNCS, 2008, Vol. 5209, pp. 100-112.

11. Childs A., Jao D., Soukharev V. Constructing elliptic curve isogenies in quantum subexponential time, *Math. Cryptol*, 2014, Vol. 8 (1), pp. 1-29.

12. Feo L. de, Jao D., Plut J. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, *Post-Quantum Cryptography*, LNCS, 2011, Vol. 7071, pp. 19-34.

13. Rostovtsev A. G., Makhovenko E. B. Cryptosystem on the category of isogenous elliptic curves [Kriptosistema na kategorii izogennykh ellipticheskikh krivykh], *Problemy informatsionnoy bezopasnosti. Kompyuternye sistemy* [*Information Security Problems. Computer Systems*], 2002, no. 3, pp. 74-81.

14. Dov Gordon S., Katz J., Vaikuntanathan V. A Group Signature Scheme from Lattice Assumptions, *Cryptology ePrint archive. Report 2011/060*. Available at: https://eprint.iacr.org/2011/060.pdf (accessed 28.02.2017).

15. Laguillaumie F., Langlois A., Libert B., Stehlé D. Lattice-Based Group Signatures with Logarithmic Signature Size, *Cryptology ePrint archive. Report 2013/308*. Available at: https://eprint.iacr.org/2013/308.pdf (accessed 28.02.2017).

16. Regev O. On lattices, learning with errors, random linear codes, and cryptography, *J. ACM*, 2009, Vol. 56 (6), pp. 34:1-34:40.

17. Galbraith S., Hess F., Smart N. P. Extending the GHS Weil descent attack, *Eurocrypt 2002, LNCS*, 2002, Vol. 2332, pp. 29-44.

18. Silverman J. A bound for the Mordell–Weil rank of an elliptic surface after a cyclic base extension, *J. Algebraic Geometry*, 2000, Vol. 9, pp. 301-308.

19. Rostovtsev A. G., Makhovenko E. B. Printsip maksimalnoy odnorodnosti [Maximum homogeneity principle]//*Trudy "Metody i tekhnicheskie sredstva obespecheniia bezopasnosti informatsii [Proc. "Methods and technical tools of information security"]*, St. Petersburg, 2003, pp. 96-98.

20. Chaum D., Heijst E. van, Pfitzmann B. Cryptographically strong undeniable signatures, unconditionally secure for the signer, *Cryptology – CRYPTO'91*, LNCS, 1992, Vol. 576, pp. 470-484.

21. *GOST R 34.11-2012 Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Funktsiya kheshirovaniya* [Information Technology. Cryptographic data security. Hash Function], Moscow, Standartinform, 2013, 19 p.

22. Long D., Widgerson A. Discrete logarithm hides O (log n) bits, *SIAM J. Comput*, 1988, Vol. 17, pp. 363-372.

23. Debiao H., Jianhua C., Jin H. A Random number generator based on isogenies operations, Cryptology ePrint archive. Report 2010/094. Available at: https://eprint.iacr.org/2010/094.pdf (accessed 28.02.2017).

24. Kuan Ch. Pseudorandom Generator Based on Hard Lattice Problem, Cryptology ePrint archive. Report 2014/002. Available at: https://eprint.iacr.org/2014/002.pdf (accessed 28.02.2017).

25. Peikert C., Rosen A. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices, *Theory of Cryptography*. LNCS, 2006, Vol. 3876, pp. 145-166.

26. Zhang J., Chen Yu., Zhang Zh. Programmable Hash Functions from Lattices: Short Signatures and IBEs with Small Key Sizes, Cryptology ePrint archive. Report 2016/523. Available at: https://eprint.iacr.org/2016/523.pdf (accessed 28.02.2017).

Принцип однородности при анализе и синтезе криптографических протоколов

Александрова Е. Б.
Санкт-Петербургский политехнический университет Петра Великого
Санкт-Петербург, Россия
helen@ibks.spbstu.ru

Аннотация. **Рассматривается принцип сложностной однородности для анализа и синтеза криптографических протоколов. Приведено сравнение двух протоколов аутентификации в соответствии с указанным принципом. Предложены способы снижения сложностной неоднородности в протоколе цифровой подписи.**

Ключевые слова: **криптографический протокол, цифровая подпись, задача дискретного логарифмирования на эллиптической кривой, сложностная однородность.**

Литература

1. Ростовцев А. Г. Теоретическая криптография / А. Г. Ростовцев, Е. Б. Маховенко. – СПб.: Профессионал, 2005. – 480 с.

2. Rivest R. L. A method for obtaining digital signatures and public-key cryptosystems / R. L. Rivest, A. Shamir, L. Adleman // Communications of the ACM. – 1978. – Vol. 21, no. 2. – P. 120–126.

3. Rabin M. Digitalized signatures and public key functions as intractable as factorization / M. Rabin // MIT Lab. for Comput. Sci. – Technical Report MIT/LCS/TR-212, 1979.

4. Fiat A. How to prove yourself: Practical solutions to identification and signature problems / A. Fiat, A. Shamir // Cryptology – CRYPTO'85. – LNCS. – 1990. – Vol. 263. – P. 186–194.

5. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms / T. ElGamal // IEEE Trans. Inf. Theory. – 1985. – Vol. IT-31. – P. 469–472.

6. Diffie W. New directions in cryptography / W. Diffie, M. Hellman // IEEE Trans. Inf. Theory. – 1976. – Vol. IT-22. – P. 644–654.

7. ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – М.: Стандартинформ, 2013. – 29 с.

8. Buchmann J. Cryptography based on number fields with large regulator / J. Buchmann, M. Maurer, B. Moller // J. de Théorie des Nombres de Bordeaux. – 2000. – Vol. 12, no. 2. – P. 293–307.

9. Chor B. A knapsack-type public key cryptosystem based on arithmetic in finite fields / B. Chor, R. Rivest // IEEE Trans. Inf. Theory. – 1988. – Vol. IT-34. – P. 901–909.

10. Bröker R. Evaluating large degree isogenies and applications to pairing based cryptography / R. Bröker, D. Charles, K. Lauter // Pairing-Based Cryptography – Pairing 2008. – LNCS. – 2008. – Vol. 5209. – P. 100–112.

11. Childs A. Constructing elliptic curve isogenies in quantum subexponential time / A. Childs, D. Jao, V. Soukharev // J. Math. Cryptol. – 2014. – Vol. 8 (1). – P. 1–29.

12. De Feo L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies / L. De Feo, D. Jao, J. Plut // Post-Quantum Cryptography. – LNCS. – 2011. – Vol. 7071. – P. 19–34.

13. Ростовцев А. Г. Криптосистема на категории изогенных эллиптических кривых / А. Г. Ростовцев, Е. Б. Маховенко // Проблемы информационной безопасности. Компьютерные системы. – 2002. – № 3. – С. 74–81.

14. Dov Gordon S. A Group Signature Scheme from Lattice Assumptions / S. Dov Gordon, J. Katz, V. Vaikuntanathan // Cryptology ePrint archive. Report 2011/060. – URL: https://eprint.iacr.org/2011/060.pdf (дата обращения: 28.02.2017).

15. Laguillaumie F. Lattice-Based Group Signatures with Logarithmic Signature Size / F. Laguillaumie, A. Langlois, B. Libert, D. Stehlé // Cryptology ePrint archive. Report 2013/308. – URL: https://eprint.iacr.org/2013/308.pdf (дата обращения: 28.02.2017).

16. Regev O. On lattices, learning with errors, random linear codes, and cryptography / O. Regev // J. ACM. – 2009. – Vol. 56 (6). – P. 34:1–34:40.

17. Galbraith S. Extending the GHS Weil descent attack / S. D. Galbraith, F. Hess, N. P. Smart // Eurocrypt 2002. – LNCS. – 2002. – Vol. 2332. – P. 29–44.

18. Silverman J. A bound for the Mordell–Weil rank of an elliptic surface after a cyclic base extension / J. H. Silverman // J. Algebraic Geom. – 2000. – Vol. 9. – P. 301–308.

19. Ростовцев А. Г. Принцип максимальной однородности / А. Г. Ростовцев, Е. Б. Маховенко // Методы и технические обеспечения безопасности информации: тр. конф. – СПб., 2003. – С. 96–98.

20. Chaum D. Cryptographically strong undeniable signatures, unconditionally secure for the signer / D. Chaum, E. van Heijst, B. Pfitzmann // Cryptology – CRYPTO'91. – LNCS. – 1992. – Vol. 576. – P. 470–484.

21. ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования. – М.: Стандартинформ, 2013. – 19 с.

22. Long D. Discrete logarithm hides O (log n) bits / D. Long, A. Widgerson // SIAM J. comput. – 1988. – Vol. 17. – P. 363–372.

23. Debiao H. A Random number generator based on isogenies operations / H. Debiao, C. Jianhua, H. Jin // Cryptology ePrint archive. Report 2010/094. – URL: https://eprint.iacr.org/2010/094.pdf (дата обращения: 28.02.2017).

24. Kuan Ch. Pseudorandom Generator Based on Hard Lattice Problem / Ch. Kuan // Cryptology ePrint archive. Report 2014/002. – URL: https://eprint.iacr.org/2014/002.pdf (дата обращения: 28.02.2017).

25. Peikert C. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices / C. Peikert, A. Rosen // Theory of Cryptography. – LNCS. – 2006. – Vol. 3876. – P. 145–166.

26. Zhang, J. Programmable Hash Functions from Lattices: Short Signatures and IBEs with Small Key Sizes / J. Zhang, Yu Chen, Zh. Zhang // Cryptology ePrint archive. Report 2016/523. – URL: https://eprint.iacr.org/2016/523.pdf (дата обращения: 28.02.2017).

Аппроксимация нечетких моделей приведенными полиномами над конечными полями Галуа

Фомичева С. Г.
Норильский государственный индустриальный институт
Норильск, Россия
levikha@rambler.ru

Аннотация. **Приведены доказательства утверждений, которые позволяют выполнять изоморфные преобразования классических аддитивных нечетких моделей, функционирующих в поле вещественных чисел, в их аналоги, способные функционировать в конечных полях Галуа. Существование таких изоморфных преобразований обусловливает возможность адекватного квантования баз знаний, представленных в виде аддитивных нечетких и нейро-нечетких систем. Способность функционирования в конечных полях и в их расширениях, в свою очередь, позволяет адекватно применять к ним механизмы защиты информации на базе теории помехоустойчивого кодирования и теории криптографии.**

Ключевые слова: **аддитивные нечеткие модели, мультиагентные телекоммуникационные системы, изоморфизм, квантование, конечные поля Галуа, приведенные полиномы над конечными полями.**

Введение

Интенсивное развитие беспроводных и мобильных сетей связи, распределенных информационно-телекоммуникационных систем и, в частности, открытых мультиагентных систем (ОМАС) приводит к формированию новых концептуальных сущностей, например, таких как агенты, которыми необходимо управлять в реальном времени [1]. В январе 1997 г. язык нечеткого управления FCL (*fuzzy control language*) внесен в Международный стандарт программируемых контроллеров IEC 1131-7.

При росте количества узлов распределенной информационно-телекоммуникационной системы, числа и разновидностей агентов, мигрирующих в ОМАС, возникает комплекс проблем: необходимость обеспечения целостности информации, переносимой агентами, обеспечение непротиворечивого обмена информацией между агентами, а также возможность адекватного пополнения баз данных и знаний агентов на пути их миграции.

В частности, рассматривая в составе ОМАС функционирование управляющих и автономных агентов, реализующих задачи обобщения данных и знаний, выделим этап предварительной обработки информации, предшествующий этапу передачи информации по распределенным каналам связи. Одна из важных на данном этапе задач, которые приходится решать агенту, – оптимизация параметров *квантования* информации. И если задачам квантования данных при теоретических исследованиях и практических реализациях уделялось достаточное внимание, то вопросы квантования *знаний* ни в отечественной, ни в зарубежной литературе в должной мере не освещены. Оптимизируемыми параметрами при квантовании знаний, представленных в виде аддитивных нечетких моделей, могут выступать, например, количество значимых правил базы знаний, термов лингвистических переменных, параметров адаптации каждого лингвистического терма, уровней иерархии аддитивной нечеткой модели, точность обобщения. Выбранные параметры квантования знаний, очевидно, определяют объем транспортируемой мобильными агентами базы знаний, скорость ее адаптации и модификации, возможность применения конкретных механизмов защиты структуры базы знаний и ее содержимого.

Также следует отметить, что уровень защиты знаний должен быть выше уровня защиты данных, на основе которых эти знания сформированы. То есть возникает необходимость в построении *иерархических* систем защиты как знаний, так и данных. Конструктивные подходы к созданию иерархических систем защиты информации существуют [2, 3] и, как правило, реализуются алгебраическими механизмами в конечных полях Галуа. Следовательно, структура транспортируемой базы знаний и ее содержимое должны быть подготовлены для адекватного применения к ним иерархических механизмов защиты. В частности, база знаний после ее *квантования* может быть представлена в виде изоморфных концептуальных сущностей, например, таких как *полиномы* над конечными полями Галуа.

В данной статье докажем основные утверждения, которые обусловливают возможность изоморфных преобразований классических аддитивных нечетких сетей, функционирующих в поле вещественных чисел, в их аналоги, реализованные в конечных полях Галуа. Представление аддитивных нечетких сетей в виде полиномов над конечными полями и их расширениями, в свою очередь, позволяет адекватно применять к ним механизмы защиты информации на базе теории помехоустойчивого кодирования и теории криптографии.

1. Аппроксимация аддитивных нечетких моделей полиномиальными функциями над полем вещественных чисел

Доказаны теоремы об универсальной аппроксимации нечетких продукционных моделей полиномами над полями вещественных чисел [4–7]. Доказательства этих теорем опираются на теоремы Вейерштрасса и Вейерштрасса – Стоуна в том смысле, что в основе этой универсальной аппроксимации лежит способность аддитивных нечетких моделей аппроксимировать любую полиномиальную функцию, ко-

торой, в свою очередь, можно аппроксимировать любую непрерывную функцию.

Приведем здесь без доказательства теоремы Вейерштрасса и Вейерштрасса – Стоуна [8].

Теорема 1.1 (Вейерштрасса). Пусть $f(x)$ – непрерывная функция, определённая на отрезке $[a,b]$. Тогда для любого $\varepsilon > 0$ существует такой многочлен $p(x)$ с вещественными коэффициентами, что для любого $x \in [a,b]$ выполнено условие

$$|f(x) - p(x)| < \varepsilon.$$

Теорема 1.2 (Вейерштрасса – Стоуна). Пусть $C(X)$ – кольцо непрерывных функций на бикомпакте X с топологией равномерной сходимости, порожденной нормой

$$\|f(x)\| = \max_{x \in X} |f(x)|, \quad f(x) \in C(X),$$

и пусть $C_0 \subseteq C(x)$ есть подкольцо, содержащее все константы и разделяющее все точки из X, т. е. для любых двух различных точек $x_1 \in X$ и $x_2 \in X$ существует функция $f(x) \in C_0$, для которой $f(x_1) \neq f(x_2)$. Тогда $[C_0] = C(x)$, т. е. всякая непрерывная функция на X есть предел равномерно сходящейся последовательности функций из C_0.

А также приведем формулировку и доказательство теоремы Коско [5] (в силу отсутствия такового в русскоязычных изданиях).

Теорема 1.3 (Коско). Аддитивная нечеткая система F универсально аппроксимирует функцию $f(X) \to Y$, если множество X компактно и функция $f(X)$ непрерывна на этом компакте.

Доказательство

Пусть $\varepsilon > 0$ – некоторая малая величина. Требуется доказать, что $|F(x) - f(x)| < \varepsilon$ для всех $x \in X$, X – компактное подмножество R^n. $F(x)$ – центроид выходной лингвистической переменной аддитивной нечеткой системы F.

Поскольку непрерывность $f(X)$ на компакте X определяет универсальную непрерывность, существует некоторое фиксированное расстояние d, такое, что для всех x и z в X, $|f(x) - f(z)| < \frac{\varepsilon}{4}$, если $|x - z| < d$. Построим цепь открытых кубов $M_1, ..., M_m$, которые покрывают X таким образом, что это приводит к наложению их в координатах n так, что каждый угол куба находится в центре c_j его соседа M_j.

Пусть B_j – симметричное нечеткое множество, сосредоточенное над $f(c_j)$. Тогда $f(c_j)$ есть центр (высота) нечеткого множества B_j.

Пусть $u \in X$. Тогда конструкция u содержит самое большее 2^n перекрывающихся открытых куба M_j.

Пусть w – любой куб в том же множестве. Если $u \in M_j$ и $w \in M_k$, то для всех $v \in M_j \cap M_k$ имеем $|u - v| < d$ и $|u - w| < d$. Универсальная непрерывность подразумевает, что

$$|f(u) - f(w)| \le |f(u) - f(v)| + |f(v) - f(w)| < \frac{\varepsilon}{2}.$$

Тогда для центров кубов c_j и c_k имеем

$$|f(c_j) - f(c_k)| < \frac{\varepsilon}{2}.$$

Пусть $x \in X$. Тогда x также находится самое большее в 2^n открытых кубах с центрами c_j и

$$|f(c_j) - f(x)| < \frac{\varepsilon}{2}.$$

По k-й координате ограниченного пространства R^p устанавливается k-я высота (центр) элемента аддитивной системы $F(x)$, которая лежит либо «на», либо «между» k-й высоте (центре) компоненты B_j.

Так как $|f(c_j) - f(c_k)| < \frac{\varepsilon}{2}$ для всех $f(c_j)$,

$$|F(x) - f(c_j)| < \frac{\varepsilon}{2}.$$

Тогда

$$|F(x) - f(x)| \le |F(x) - f(c_j)| + |f(c_j) - f(x)| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

■

Доказательство теоремы Коско показывает, что нечеткие множества A_i и B_j можно заменить совокупностью конечных векторов $(a_1^i, ..., a_n^i)$ и $(b_1^j, ..., b_p^j)$. Дискретный вариант B_j должен иметь высоту «в» или «близко» к центроиду B_j. Таким образом, всегда можно работать с большемерными гиперкубами, рассматривая нечеткие правила или продукции как картографическую матрицу (или нечеткую реляционную базу знаний) между гиперкубами как точки в еще большем гиперкубе.

Конструктивным результатом доказательства этих теорем является оценка необходимого количества правил модели для заданной точности аппроксимации, которое определяется с помощью минимального расстояния между центроидами двух смежных нечетких множеств, представляющих заключения правил, обозначаемых как y_i и y_{i+1}:

$$|y_i - y_{i+1}| < \frac{\varepsilon}{2^g - 1}, \qquad (1)$$

где ε – точность аппроксимации; g –максимальное число перекрытий (*overlapping*) нечетких множеств входных переменных на компактном множестве X (для одной входной переменной $g = 2$).

Для одной входной переменной необходимое количество правил определяется выражением

$$n \ge \frac{|X|}{\varepsilon}.$$

Очевидно, что при стремлении ε к нулю количество правил неограниченно, но для заданного значения ε количество правил может быть оценено с помощью (1).

Однако данные результаты не дают ответов на вопросы, какую конкретно нечеткую модель необходимо выбрать, сколько должно быть правил для аппроксимации заданной функции, каковы механизмы регулирования точности аппроксимации, также остается нерешенной проблема компактной упаковки аддитивной нечеткой модели в ограниченное адресное пространство.

2. Аппроксимация аддитивных нечетких моделей приведенными полиномами над конечными полями

В текущем параграфе докажем основные утверждения, позволяющие обосновать и реализовать механизмы

мягкой иерархической консолидации знаний агентов и надежного хранения данных агентов в информационно-телекоммуникационных ОМАС. Для этого следует обосновать возможность создания аналогов нечетких и нейро-нечетких структур, адекватно функционирующих в конечных полях.

Теорема 2.1. Аддитивная нечеткая система F со сколь угодно малой точностью $\varepsilon > 0$ аппроксимирует полином с вещественными коэффициентами $p(x) \to Y$, если множество X компактно.

Доказательство

В силу верности теоремы Коско имеем, что аддитивная нечеткая система F универсально аппроксимирует непрерывную функцию $f(x) \to Y$ на компактном множестве X, если эта функция непрерывна на этом компакте, т. е.

$$\left|F(x) - f(x)\right| < \varepsilon_1,$$

где $\varepsilon_1 > 0$ – сколь угодно малая величина; $x \in X$.

В соответствии с теоремой Вейерштрасса, любая непрерывная функция $f(x)$, определённая на компакте X, может быть аппроксимирована с точностью ε_2 многочленом $p(x)$ с вещественными коэффициентами, т. е. для $\forall x \in X$ выполнено условие $\left|f(x) - p(x)\right| < \varepsilon_2$.

Тогда

$$\left|F(x) - f(x)\right| = \left|F(x) - (p(x) \pm \varepsilon_2)\right| =$$

$$= \left|F(x) - p(x) \mp \varepsilon_2\right| < \varepsilon_1;$$

$$\left|F(x) - p(x)\right| < \left|\varepsilon_1 \pm \varepsilon_2\right|.$$

Положив $\varepsilon = \left|\varepsilon_1 - \varepsilon_2\right|$, получаем требуемое утверждение

$$\left|F(x) - p(x)\right| < \varepsilon. \quad \blacksquare$$

Для доказательства иных аппроксимирующих свойств аддитивных нечетких и адаптивных нейро-нечетких систем потребуются ряд известных утверждений (2.1–2.7). Необходимость в этих утверждениях возникает в связи требованием перехода из вещественного поля вычислений в поле вычислений над конечными полями. Отметим, что обычной дискретизацией вещественных чисел в множество целых чисел проблемы масштабирования баз знаний решить нельзя, так как множество целых чисел не является полем (в нем отсутствует мультипликативно обратный элемент). Вычисления в конечных полях повсеместно используются в теории кодирования и в теории криптографии, без которых, в свою очередь, невозможно обосновать параметры надежной передачи информации в каналах связи ОМАС ИТКС.

Конечное поле – поле, число элементов которого конечно. Если число элементов поля является степенью q^m – некоторого натурального простого числа q, являющегося характеристикой этого поля, то такое поле называют полем Галуа и обозначают $GF(q^m)$.

Известно [9, 10], что для $\forall q$ и $\forall m \in N$, где N – множество натуральных чисел, существует единственное (с точностью до изоморфизма) поле из q^m элементов. Количество элементов поля называют *порядком* этого поля и обозначают $card(GF(q^m))$.

Также известны утверждения 2.1–2.7 [9]:

Утверждение 2.1 [10]

Поле $GF(q^n)$ содержит подполе $GF(q^m)$ в том, и только в том случае, если $n \mid m$ (m делит n). В частности, в любом $GF(q^m)$ содержится $GF(q)$, называемое *простым* полем.

Утверждение 2.2 [10]

Поле $GF(q)$ изоморфно полю $Z \mid (q)$ – классов вычетов кольца целых чисел по модулю q.

Любое конечное расширение поля алгебраично [9].

Утверждение 2.3 [10]

Поле вещественных чисел R является алгебраическим замыканием Ω поля Галуа, так как всякий отличный от константы многочлен с коэффициентами из $GF(q)$ имеет по крайней мере один корень на поле вещественных чисел R.

Утверждение 2.4 [10]

В любом фиксированном *алгебраическом замыкании* Ω поля $GF(q)$ существует только одно подполе $GF(q^m)$ для каждого m. Соответствие $m \leftrightarrow GF(q^m)$ является изоморфизмом между решеткой натуральных чисел (являющихся подмножеством вещественных чисел) относительно операции делимости и решеткой конечных алгебраических расширений поля $GF(q)$, лежащих в Ω относительно включения.

Такова же решетка множества конечных алгебраических расширений любого поля Галуа, лежащего в его фиксированных алгебраическом замыкании.

Утверждение 2.5 [10]

Алгебраическое расширение $GF(q^m) / GF(q)$ является простым, т. е. $\exists \alpha \in GF(q^m)$ – примитивный элемент, такой, что $GF(q^m) = GF(q)(\alpha)$. Таким примитивным элементом α будет любой корень неприводимого многочлена степени m из кольца $GF(q)[X]$.

Утверждение 2.6 [9, 10]

Множество элементов поля $GF(q^m)$ в точности совпадает с множеством корней многочлена $X^{q^m} - X$ в Ω, т. е. $GF(q^m)$ характеризуется как подполе элементов из Ω, инвариантных относительно автоморфизма $\tau: \; x \to x^{q^m}$, называемым автоморфизмом Фробениуса.

Утверждение 2.7 [9, 10]

Если $GF(q^n) \supset GF(q^m)$, то расширение $GF(q^n) / GF(q^m)$ нормально и его группа Галуа $Gal(GF(q^n) / GF(q^m))$ циклическая порядка $n \mid m$. В качестве образующей группы $Gal(GF(q^n) / GF(q^m))$ может быть взят автоморфизм τ.

Теоремы 1.1–1.3 и утверждения 2.1–2.7 позволяют доказать следующую теорему.

Теорема 2.2 [11]

Пусть аддитивная нечеткая система F со сколь угодно малой точностью $\varepsilon_1 > 0$ аппроксимирует полином $p(x)$ с вещественными коэффициентами на компакте X.

Тогда $\exists q$ и $\exists$ полином $g(\tilde{X})$ над $GF(q^m)$ ($\tilde{x} \in \tilde{X} = \{0,1,..., q–1\}, m \in N, m > 0$), изоморфный $p(x)$, который также аппроксимирует F со сколь угодно малой точностью $\varepsilon_2 > 0$, $\varepsilon_2 = \varepsilon_1 \pm o(\varepsilon_1)$.

Доказательство

В силу верности утверждений 2.3, 2.4 устанавливается изоморфизм компакта X вещественного поля и $GF(q^m)$.

Далее в силу утверждения 2.6 имеем существование лексикографического порядка элементов $GF(q^m)$, инвариантного относительно автоморфизма Фробениуса, из которого

следует существование $g(\tilde{X})$ над $GF(q^m)$, $\tilde{x} \in \{0,1,...,q-1\}$ и изоморфизм $p(X) \leftrightarrow g(\tilde{X})$. ■

В теореме 2.2 говорится о существовании полинома $g(\tilde{X})$ над $GF(q^m)$, который с заданной точностью аппроксимирует аддитивную нечеткую систему F, но не устанавливается вид этого полинома. Чтобы указать вид этого полинома, введем в рассмотрение ряд обозначений и ограничений.

Пусть $x = (x_1, x_2, ..., x_m)$ – вектор нечетких входных переменных $x \in X$; y – нечеткая выходная переменная аддитивной нечеткой системы F, $y \in Y$.

Пусть q – некоторое априорно заданное простое число.

Ограничение 2.1

Пусть $A^{(i)} = \{A_1^{(i)}, A_2^{(i)}, ..., A_q^{(i)}\}$ – множество лингвистических термов нечеткой входной переменной x_i, заданных на X соответствующими нечеткими множествами с функциями принадлежности $\mu_{A_l}(x_i) \in [0,1]$ для $l = \overline{1,q}$. A – множество лингвистических термов вектора $x = (x_1, x_2, ..., x_m)$:

$$A = A^{(1)} \times A^{(2)} \times ... \times A^{(m)}.$$

Ограничение 2.2

Пусть $B = \{B_1, B_2, ..., B_q\}$ – множество лингвистических термов, заданных на Y соответствующими нечеткими множествами с функциями принадлежности $\mu_{B_z}(y) \in [0,1]$ для $z = \overline{1,q}$.

Ограничение 2.3

Пусть каждая функция принадлежности $\mu_{A_l}(x_i) \in [0,1]$ для $l = \overline{1,q}$ и $\mu_{B_z}(y) \in [0,1]$ для $z = \overline{1,q}$ является симметричной и имеет центроиды $x_i^{(l)}$ с вершинами в точках с абсциссами $\frac{l-1}{q}$ и основаниями

$$\left[0, \frac{1}{2q}\right] \text{ при } l = 1; \quad \left[1 - \frac{1}{2q}, 1\right] \text{ при } l = q;$$

$$\left[\frac{l-1}{q} - \frac{1}{2q}, \frac{l-1}{q} + \frac{1}{2q}\right] \text{ при } l \neq 1 \text{ и } l \neq q.$$

То есть ограничения 2.1 и 2.3 указывают, что характеристика поля полностью определяет расположение и количество термов.

Тогда можно доказать следующее утверждение.

Теорема 2.3

Аддитивная нечеткая система F при ограничениях 2.1–2.3 может быть аппроксимирована со сколь угодно малой точностью $\varepsilon > 0$ *приведенным* полиномом с коэффициентами над $GF(q)$.

Доказательство

Множество всех возможных паттернов $(x, y) = (x_1, x_2, ..., x_m, y)$ полностью определяют состояние и выход аддитивной нечеткой системы F, причем в силу ограничения 2.1 количество различных векторов $x = (x_1, x_2, ..., x_m)$ ограничено и составляет $\|A\| = q^m$.

Введение ограничений 2.3 на положение центроидов и размах оснований функций принадлежности обеспечивает *непрерывное* покрытие компакта X *упорядоченными* лингвистическими термами, что дает возможность применять теорему Коско и, следовательно, теоремы 2.1 и 2.2.

Тогда векторы $x = (x_1, x_2, ..., x_m)$ аддитивной нечеткой системы F могут быть изоморфно отображены в конечное поле $GF(q^m)$, а сама F с использованием ограничения 2.2 полностью задана ее таблицей истинности для многозначной логики.

Число строк в таблице истинности равно $card(GF(q^m))$ и однозначно связано с мощностью базы правил для заданной точности аппроксимации, которое определяется с помощью минимального расстояния между центроидами двух смежных нечетких множеств, представляющих заключения правил.

Известно, что булевская функция, заданная ее таблицей истинности, может быть представлена полиномом Жегалкина, а для q-значной логики функция, заданная таблицей ее значений, – приведенным полиномом с коэффициентами в $GF(q)$ тогда и только тогда, когда q – простое [12, 13].

Следовательно,

$$\left|F(x) - p(x)\right| = \left|F(\tilde{x}) - q(\tilde{x})\right| < \varepsilon,$$

где $F(\tilde{x})$ – изоморфное отображение F в $GF(q^m)$ для априорно заданного q, определяющего количество термов в ее нечетких переменных,

$$g(\tilde{x}) = a_0 \oplus \sum a_i \tilde{x}_i \oplus \sum a_{ij} \tilde{x}_i \tilde{x}_j \oplus ... \oplus a_{12...m} x_1 x_2 ... x_m, \quad (2)$$

где $g(\tilde{x})$ – приведенный многочлен над $GF(q)$, a_i, a_{ij}, ..., $a_{12...m} \in GF(q)$, $\tilde{x} \in GF(q), i = \overline{1,m_i}$. ■

Алгоритмы формирования приведенных полиномов аналогичны алгоритмам построения полиномов Жегалкина, среди последних наиболее эффективные приведены в [13, 14], что уже само по себе приближает решение задачи автоматического формирования *полной* базы знаний агента.

Число слагаемых приведенного полинома (2) определяется количеством различных мономов (элементарных конъюнкций при $q = 2$), которые в свою очередь являются элементарными правилами. Приведем нижние и верхние оценки сложности формирования функций в классе приведенных полиномов и *приближенных* приведенных полиномов.

3. Оценки сложности формирования функций в классе приведенных полиномов над конечными полями

Введем ряд обозначений для оценки сложности функций в классе полиномов [13].

Множество всех функций многозначной логики с основанием q обозначим P_q. Пусть $l(G)$ обозначает количество слагаемых полинома G и называется длиной полинома G.

Пусть $f(x_1, x_2, ..., x_m) \in P_q$ и имеет соответствующий ей приведенный полином G_f над P_q.

Введем функционал

$$l_G(f) = \min(l(G_f)),$$

обозначающий длину полинома G_f. Значение $l_G(f)$ называют *сложностью функции f в классе приведенных полиномов.*

Также введем в рассмотрение функцию

$$L_G(m) = \max_{f \in P_q(m)} (l_G(f)),$$

которая характеризует сложность «самой сложной функции» от m-переменных в классе приведенных полиномов. Функ-

ция $L_G(m)$ называется *функцией Шеннона сложности в классе приведенных полиномов.*

Тогда можно доказать следующие утверждения для нижней и верхней оценок сложности функций.

Теорема 3.1

Нижняя оценка для функции Шеннона сложности в классе приведенных полиномов над $GF(q)$ задается неравенством

$$L_G(m) \geq \frac{q^m}{m \log_q (q+1)}.$$

Доказательство

Пусть $L_G(m) = L$. Всего существует $(q+1)^m$ мономов (элементарных конъюнкций при $q = 2$) от m-переменных, поэтому количество полиномов длины не больше L от m переменных не превосходит $((q+1)^m)^L$. Число функций P_q от m переменных равно q^{q^m}. Очевидно, что количество полиномов не может быть меньше числа функций, иначе найдется функция, для которой не существует эквивалентного ей полинома длины $\leq L$, что противоречит определению $L_G(m)$. Следовательно,

$$(q+1)^{mL} \geq q^{q^m}.$$

Выразив L из данного неравенства, получаем

$$L_G(m) \geq \frac{q^m}{m \log_q (q+1)}. \blacksquare \qquad (3)$$

Оценку сверху для $L_G(m)$ можно получить, обобщив на случай многозначной логики верхнюю оценку для булевских функций. А именно [13]

$$L_{P_2}(m) \leq 2 \cdot \frac{2^m}{m}(1 + \ln(m)).$$

Тогда для приведенного полинома в P_q получим

$$L_G(m) \leq \frac{q^{m+1}}{m}(1 + \ln(m)). \qquad (4)$$

Как видно из выражений (3) и (4), при аппроксимации аддитивных нечетких систем приведенными полиномами над $GF(q^m)$ по-прежнему, как и в классических нечетких продукционных моделях, имеет место экспоненциальный рост количества правил при стремлении к нулю ошибки аппроксимации, что приводит к существенному росту вычислительной сложности и практической неприменимости.

С практической точки зрения достаточно иметь приемлемую для адекватного принятия решения точность аппроксимации. В этом случае задача сводится к поиску компромисса между указанной точностью и количеством правил модели. Подходы к поиску такого компромисса могут быть следующими:

1) использовать алгоритмы формирования *приближенных* приведенных полиномов;

2) модифицировать известные имеющиеся рекурсивные алгоритмы, базирующиеся на формировании эквивалентных генераторов *m*-последовательностей (последовательностей максимальной длины);

3) строить иерархические конструкции из адаптивных нечетких систем или их изоморфных образов над конечными полями, используя возможность представления приведенного полинома в виде произведения его неприводимых сомножителей.

Первый подход при его классической реализации позволяет снизить сложность формирования приближенного приведенного полинома по сравнению с исходным на порядок. Покажем это.

Понятие приближенного полинома базируется на использовании некоторой действительной константы $\delta \in [0,1]$, которая обозначает долю наборов, на которых значения полиномов $g_1(\tilde{x}^m)$ и $g_2(\tilde{x}^m)$ различаются в смысле расстояния Хэмминга $d(g_1, g_2)$. То есть говорят, что полином $g_1(\tilde{x}^m)$ является δ-приближением полинома $g_2(\tilde{x}^m)$, если $\frac{d(g_1, g_2)}{q^m} \leq \delta$ (для полинома Жегалкина $q = 2$). Иными словами, доля совпадений между значениями $g_1(\tilde{x}^m)$ и $g_2(\tilde{x}^m)$ должна быть не менее $1 - \delta$.

В частности, верхние и нижние оценки функций сложности над классом приближенных приведенных полиномов могут быть также получены обобщением известных оценок для полиномов Жегалкина, последние из которых приведены в [13].

Для оценки сложности приближенных полиномов введены в рассмотрение четыре функции сложности:

$r_\delta(g) = \min\limits_{g1-\delta-g2} r(P_q)$ – ранг приближенного полинома g (число сомножителей максимального монома);

$l_\delta(g) = \min\limits_{g1-\delta-g2} l(P_q)$ – длина приближенного полинома g;

$l_\delta(m) = \max\limits_{g1-\delta-g2} l_q(g)$ – функция Шеннона сложности в классе приближенных приведенных полиномов;

$r_\delta(m) = \max\limits_{g1-\delta-g2} r_q(g)$ – асимптотика ранга приближенного полинома g.

Опуская громоздкие умозаключения [13], приведем верхние оценки для двух последних функций:

$$l_\delta(m) = q^m \text{ при } \delta = 0;$$

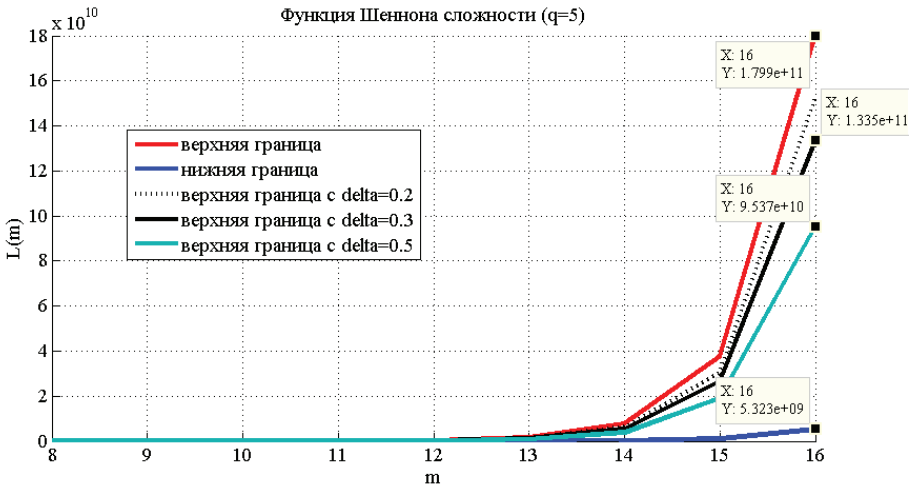
$$l_\delta(m) \leq \frac{q-1}{q}(1-\delta) \cdot q^m + 1 \text{ при } \delta \in \left(0, \frac{1}{2}\right);$$

$$r_\delta(m) = m \text{ при } \delta = 0;$$

$$r_\delta(m) \sim \frac{q-1}{q} \cdot m \text{ при } \delta \in \left(0, \frac{1}{2}\right).$$

На рисунке приведены графики функций Шеннона сложности для характеристики поля $q = 5$. Видно, что при $m \geq 16$ число мономов даже *приближенного* приведенного полинома весьма велико (транспортировка такого полинома потребует около 100 тысяч агентов при условии, что каждый агент транспортирует 1000 мономов). При необходимости транспортировки *полной* базы правил в виде такого «длинного» приведенного полинома потребуется его дополнительная обработка – обратимая свертка (например, алгоритмом Берлекэмпа – Месси).

Наличие целевой функции у агента позволяет добиться *регулируемого баланса* между количеством правил и точностью аппроксимации, формируя *иерархические* нечеткие продукционные модели (аддитивные *m*-входные иерархические нечеткие модели), включающие в себя $(m-1)$-входные нечеткие продукционные модели [15]. Иерархическая схема



Границы функций сложности Шеннона при построении приведенных полиномов над конечными полями

при этом, очевидно, должна учитывать рейтингование вложенных в нее нечетких моделей (рейтинговые механизмы в данной статье не рассматриваются).

Докажем, что аддитивные m-входные *иерархические* нечеткие модели также являются универсальными аппроксиматорами. Для этого следует показать, что вид полинома, аппроксимирующего аддитивную нечеткую модель, может быть представлен некоторой иерархической структурой. Иерархическая структура, в свою очередь, всегда может быть получена из мультипликативной формы полинома.

Поэтому на основании теорем Коско и Вейерштрасса может быть сформулировано следующее утверждение.

Теорема 3.2

Существует полином $p(X) \to Y$ с вещественными коэффициентами и с мультипликативной структурой своих одночленов, который аппроксимирует аддитивная нечеткая система F со сколь угодно малой точностью $\varepsilon > 0$, если множество X компактно.

Доказательство

Возможность представления произвольного полинома в виде мультипликативной структуры его членов вытекает из существования интерполяционной формулы Лагранжа, а также непосредственно из утверждений теорем 2.1–2.3, Вейерштрасса и Коско. Формула Лагранжа в данном случае имеет вид

$$f(x_1,...,x_m) = \\ = \sum_{(a_1a_2...a_m)} f(a_1a_2...a_m)(x_1 + a_1 + 1)...(x_m + a_m + 1). \quad \blacksquare$$

Как аддитивная, так и мультипликативная форма приведенного полинома, который является образом аддитивной нечеткой модели, позволяет распределять (и перераспределять) его мономы (элементарные дизъюнкции и конъюнкции при $q = 2$) между отдельными агентами, объединенными в одну группу для выполнения целевой функции. Целевая функция представляет собой не что иное, как полную (или полную с заданной точностью аппроксимации) форму приведенного полинома (аддитивную или мультипликативную).

В целом отметим, что иерархические адаптивные нейро-нечеткие модели, представленные приведенными полиномами, позволяют реализовать принципы распределенности многоагентных систем, а их практическое воплощение [15] подтверждает эффективность функционирования в распределенных производственных информационно-телекоммуникационных системах.

Заключение

В данной статье на основании теорем об универсальной аппроксимации нечетких продукционных моделей, опирающихся на доказательствах теорем Вейерштрасса, Вейерштрасса – Стоуна, а также теоремы Коско доказана теорема о существовании фиксированного простого числа q, при котором аддитивная нечеткая система F с симметричными функциями принадлежности для ее входных x_i и выходной переменной y на компакте X может быть аппроксимирована со сколь угодно малой точностью ε *приведенным* полиномом (естественным обобщением полинома Жегалкина для многозначной логики).

Приведены верхние и нижние оценки функций Шеннона сложности для точных и приближенных приведенных полиномов над конечными полями Галуа. Показана возможность аппроксимации иерархических нечетких и нейро-нечетких систем приведенными полиномами над конечными полями Галуа.

Полученные в статье доказательства могут быть использованы при решении задач автоматического квантования баз знаний, реализованных в виде аддитивных нечетких и нейро-нечетких сетей, что особенно важно при разработке интеллектуальных агентов ОМАС распределенных информационно-телекоммуникационных систем.

Литература

1. Тимофеев А. В. Интеллектуализация процессов управления и навигации робототехнических систем / А. В. Тимофеев, Р. М. Юсупов // Робототехника и техническая кибернетика. – 2014. – № 2 (3). – С. 19–22.

2. Pat. USA 7532724 H04L 9/00. Method for encrypting and decrypting data for multi-level access control in an ad-hoc network. Bezzateev S., Jung Tae-chul, Lee Kyung-hee, Krouk E., Sitalov A.

3. Фомичева С. Г. Защита информации в распределенных иерархических системах / С. Г. Фомичева // Науч.-технич. ведомости СПбГТУ. Информатика, телекоммуникации, управление. – 2008. – № 2. – С. 91–97.

4. Борисов В. В. Нечеткие модели и сети / В. В. Борисов, А. С. Круглов, А. С. Федулов. – М.: Горячая линия – Телеком, 2012. – 284 с.

5. Kosco B. Fuzzy system as universal approximators / B. Kosco // Proc. of IEEE Int. Conf. on Fuzzy Systems. – San Diego, 1992. – P. 1153–1162.

6. Wang L. X. Fuzzy systems are universal approximators / L. Wang // Proc. of IEEE Int. Conf. on Fuzzy Systems. – San Diego, 1992. – P. 1163–1169.

7. Ying H. Sufficient conditions on uniform approximation of multivariate functions by general Takagi-Sugeno fuzzy systems with linear rule consequents / H. Ying // IEEE Trans. Systems, Man and Cybernetics. Part A. – 1998. – Vol. 28, no. 4. – P. 515–520.

8. Фихтенгольц Г. М. Курс дифференциального и интегрального исчисления. В 3 т. Т. 1 / Г. М. Фихтенгольц. – М.: Физматлит, 2003. – 680 с.

9. Лидл Р. Конечные поля. В 2 т. Т. 1. / Р. Лидл, Г. Нидеррайтер; пер. с англ. – М.: Мир, 1988. – 430 с.

10. Виноградов И. М. Математическая энциклопедия / И. М. Виноградов. – М.: Сов. энциклопедия, 1977–1985. – URL: http://enc-dic.com/enc_math/Galua-pole-6052.html (дата обращения 25.01.2017).

11. Фомичева С. Г. Теория потоковых систем защиты информации / С. Г. Фомичева. – Норильск: Норильский индустр. ин-т, 2007. – 243 с.

12. Глушков В. М. Энциклопедия кибернетики. Т. 1. Жегалкина алгебра / В. М. Глушков, Н. М. Амосов, И. А. Артеменко. – URL: http://edu.sernam.ru/book_kiber1.php?id=455 (дата обращения 25.01.2017).

13. Селезнева С. Н. Булевы функции и полиномы / С. Н. Селезнева. – URL: http://mk.cs.msu.ru/images/e/ea/Bool_polynoms.pdf (дата обращения 25.01.2017).

14. Фомичева С. Г. Моделирование развития информационно-телекоммуникационных систем / С. Г. Фомичева; под ред. к.т.н., д.э.н., проф. А. В. Бабкина. – СПб.: Синтез-Бук, 2009. – 384 с.

15. Konev A. A. Adaptive control system for silicon oxide concentration in slags at processing cooper-nickel ores / A. A. Konev, S. G. Fomicheva // Software & systems. Int. Res. Practice J. – 2014. – no. 3 (107). – P. 131–141.

The Fuzzy Models Approximation are Given by Polynomials Over Finite Galois Fields

Fomicheva S. G.
Norilsk state industrial Institute
Norilsk, Russia
levikha@rambler.ru

Abstract. **Given the proofs of theorems that allow you to perform isomorphic transformations for the classical additive fuzzy networks operating in the field of real numbers to their analogs able to function on the finite Galois fields. The existence of such isomorphic transformations lead to the possibility for an adequate quantization of the knowledge bases represented as additive fuzzy and neuro-fuzzy systems. The ability to operate in finite fields and their extensions allow you to apply for them the protect information mechanisms on the theory of error-correcting coding theory and cryptography.**

Keywords: **additive fuzzy models, multi-agent telecommunication systems, isomorphism, quantization, finite Galois field, given polynomials over finite field**

References

1. Timofeev A. V., Yusupov R. M. Intellectualization of the Processes for Control and Robotic Navigation Systems [Intellektualizatsiia protsessov upravleniia i navigatsii robototekhnicheskikh sistem], *Robototekhnika i tekhnicheskaia kibernetika [Robotics and Technical Cybernetics]*, 2014, № 2 (3), pp. 19-22.

2. Patent USA 7532724 H04L 9/00. Method for encrypting and decrypting data for multi-level access control in an ad-hoc network. Bezzateev S., Jung Tae-chul, Lee Kyung-hee, Krouk E., Sitalov A.

3. Fomicheva S. G. Zaschita informatsii v raspredelennyh ierarhicheskih sistemah, *Nauchno-tehnicheskie vedomosti SPbGTU. Informatika, telekommunikatsii, upravlenie* [St. Petersburg State Polytech. Univ. J. Comput. Sci. Telecommunication and Control Systems], 2008, № 2, pp. 91-97.

4. Borisov V. V., KruglovA. S., Fedulov A. S. *Nechetkie modeli i seti* [Fuzzy Models and Nets], Moscow, Goryachaya Liniya Telekom, 2012, 284 p.

5. Kosco B. Fuzzy System as Universal Approximators, *Proc. of IEEE Int. Conf. on Fuzzy Systems*, San Diego,1992, pp. 1153-1162.

6. Wang L. X. Fuzzy Systems are Universal Approximators, *Proc. of IEEE Int. Conf. on Fuzzy Systems*, San Diego, 1992, pp. 1163-1169.

7. Ying H. Sufficient Conditions on Uniform Approximation of Multivariate Functions by General Takagi-Sugeno Fuzzy Systems with Linear Rule Consequents, *IEEE Transaction on Systems, Man and Cybernetics*, Part A, 1998, Vol. 28, no. 4, pp. 515-520.

8. Fikhtengol'ts G. M. *Kurs differentsial'nogo i integral'nogo ischisleniia* [Course of Differential and Integral Calculus, in 3 vol., t. 1, Moscow, Fizmatlit, 2003, 680 p.

9. Lidl R., Niederreiter H. *Konechnye polia* [FiniteFields]. Vol. 1, Moscow, Mir, 1988, 430 p.

10. Vinogradov I. M. *Matematicheskaja `entsiklopedija* [Mathematical Encyclopedia], Moscow, Sovetskaja `entsiklopedija, 1977–1985. Available at: http://enc-dic.com/enc_math/Galua-pole-6052.html (accessed 25 January 2017).

11. Fomicheva S. G. *Teoriia potokovykh sistem zashchity informatsii* [The Stream Systems Theory for Information Protection], Norilisk, Norilskii industrialniy institut, 2007, 243 p.

12. Glushkov V. M., Amosov N. M., Artemenko I. A. *Entsiklopedija kibernetiki* [Encyclopedias of Cybernetics]. T. 1. Zhegalkina algebra [Zhelgalkin Algebra]. Available at: http://edu.sernam.ru/book_kiber1.php?id=455 (accessed 25 January 2017).

13. Selezneva S. N. *Bulevy functsii i polinomy* [The Boolean Functions and Polynomial's]. Available at: http://mk.cs.msu.ru/images/e/ea/Bool_polynoms.pdf (accessed 25 January 2017).

14. Fomicheva S. G. et. al. *Modelirovanie razvitiia informatsionno-telekommunikatsionnykh sistem* [The Simulation of the Development for Information and Telecommunication Systems], ed. A. V. Babkin. St. Petersburg, Sintez-Buk, 2009, 384 p.

15. Konev A. A., Fomicheva S. G. Adaptive Control System for Silicon Oxide Concentration in Slags at Processing Cooper-nickel Ores [Software & systems Int. Res. practice J], 2014, no. 3 (107), pp. 131-141.

Система показателей качества мониторинга технологических процессов в ракетно-космической отрасли

Шмелев В. В.
Военно-космическая академия им. А. Ф. Можайского
Санкт-Петербург, Россия
valja1978@yandex.ru

Аннотация. **В статье предлагается специализированная четырехуровневая система показателей качества для комплексного оценивания мониторинга функционирования пневмогидравлической системы ракеты-носителя «Союз-2». Система содержит 13 показателей нижнего уровня и 6 показателей верхних уровней. В отличие от существующих аналогов и рекомендаций, все показатели в системе количественные. Благодаря этому достигается объективность оценки. Полнота оценки обеспечивается включением в систему эксплуатационных показателей, показателей сопровождения и результативности. По предлагаемой системе оценивается качество мониторинга с использованием вариантов программного обеспечения на основе рекурсивной модели и структурно-логического подхода, а также формируются требуемые значения показателей, удовлетворяющие специалистов-экспертов.**

Ключевые слова: **качество программного обеспечения, ракетно-космическая техника, комплексирование частных показателей, мониторинг технологического процесса, структурно-логический подход, рекурсивная модель процесса, моделирование процессов.**

Введение

Современное развитие вычислительной техники отодвигает на второй план направление в совершенствовании программного обеспечения обработки и анализа измерительной информации ракетно-космической техники (РКТ), связанное с увеличением производительности расчетов и с быстродействием ЭВМ. На первый план выдвигается направление по улучшению трудно формализуемых показателей, а именно полноты используемой информации, модифицируемости и диагностируемости уже не самого программного обеспечения (ПО), а результата его применения.

Известные работы по оцениванию качества ПО (отечественная – [1], зарубежные – [2, 3]) предлагают способы количественного оценивания некоторых показателей качества ПО и их комплексирования. На этой основе ранжируются элементы ПО, выявляются риски и увеличивается вложение ресурсов в наиболее критичные элементы, т. е. осуществляется управление процессом разработки ПО [4]. Однако в указанных работах прослеживается стремление охватить максимально широкую область применения оцениваемого ПО. При этом возникает значительная трудность использования разработанных показателей на узкоспециализированном ПО. Кроме того, в указанных работах основной упор делается на оценивание ПО как самодостаточного продукта. То есть оценивается, например, корректность кода, количество программных ошибок и т. п. При этом не уделяется должного внимания результативности применения ПО.

Настоящий материал является попыткой разработать систему показателей качества специально для предметной области обработки и анализа телеметрической информации (ТМИ) РКТ, мониторинга функционирования систем и агрегатов ракет-носителей (РН). При этом максимально конкретизируется технологический процесс, для мониторинга которого предназначено оцениваемое ПО.

Для обеспечения практической направленности разрабатываемой системы показателей она апробируется на специальном ПО (СПО) мониторинга функционирования пневмогидравлической системы (ПГС) двигательных установок (ДУ) РН «Союз-2». Кроме того, рассматривается разработанное СПО на основе оригинального структурно-логического подхода (СЛП) [5, 6]. Применяемое в настоящее время СПО мониторинга строится на основе рекурсивной модели технологического процесса. Данная модель подробно рассмотрена в [5, 7], анализ ее недостатков приведен в [5, 6].

Частные показатели качества мониторинга

Приведем краткие названия, физический смысл и формулы для вычисления частных показателей качества мониторинга технологических процессов в информационном обеспечении автоматизированной системы испытаний и применения РКТ. С целью практической осязаемости показателей они уточнены непосредственно для процессов функционирования ПГС ДУ РН «Союз-2» и обработки и анализа измерительной информации данной технической системы.

При составлении показателей использовались в том числе рекомендуемые показатели качества ПО, приведенные в [8, 9]. В указанных документах строго не регламентируется порядок вычисления показателей, приводится только их примерное содержание. При специализации показателей использовалась документация по информационному обеспечению испытаний и применения РКТ [10] и документация по РН «Союз-2» [11–13].

Предлагаемые в работе показатели специализированы для предметной области, что позволяет говорить об их адекватности запросам конечного пользователя СПО мониторинга – инженера-испытателя Информационно-аналитического центра космодрома. Применение максимально конкретной информации при формировании показателей, с одной стороны, значительно сужает область применения разработанных показателей, с другой стороны, позволяет обоснованно получить количественную характеристику каждого показате-

ля. Для других объектов мониторинга можно использовать разработанные показатели после их предварительной адаптации, что гораздо легче выполнить при наличии примера показателей хотя бы для РН «Союз-2».

В статье при формировании показателей под результатом мониторинга понимается синтезированная модель технологического процесса в виде совокупности формального описания модели и связанной с моделью формы отображения. Формой отображения является графическое представление интерфейса СПО мониторинга.

Частный показатель p_1 – точность телеметрируемых параметров (ТМП) – рассчитывается по формулам

$$p_1 = 1 - 3\sqrt{\sigma_{\text{ТМ}}^2 + \sum_{j=1}^{N_{\text{ТМП}}} \sigma^2(x_j)}\,;\ \sigma_{\text{ТМ}} = \delta_{\text{ТМ}} / 3\,;$$

$$\sigma(x_j) = \delta(x_j) / 3\,,$$

где x_j, $j = \overline{1, N_{\text{ТМП}}}$ – ТМП, используемые в СПО мониторинга; $\delta_{\text{ТМ}} = 0{,}8\ \%$ – максимальная приведенная погрешность бортовой аппаратуры с учетом «наземной» автоматизированной обработки ТМП, значение которой приведено в Программе телеизмерений, выпускаемой в комплекте технической документации на РН; $\sigma_{\text{ТМ}}$ – СКО приведенной погрешности бортовой аппаратуры с учетом «наземной» автоматизированной обработки ТМП; $\delta(x_j)$ – максимальная приведенная погрешность измерения j-го датчика, значение которой приводится в технических характеристиках датчиков, например в [14], тип датчиков – в Программе телеизмерений; $\sigma(x_j)$ – СКО приведенной погрешности измерения j-го датчика.

Показатель p_1 характеризует погрешность используемых в СПО мониторинга телеизмерений. Погрешность формируется датчиковой аппаратурой и системой сбора и обработки ТМИ. Принимается допущение о нормальном распределении погрешности. Допускается статистическая независимость телеизмерений.

Частный показатель p_2 – точность оценивания значений летно-технических характеристик (ЛТХ) – вычисляется по формулам

$$p_2 = 1 - 3\sqrt{\sum_{q=1}^{N_{\text{ЛТХ}}} \sigma^2(y_q)};\ \sigma(y_q) = \sqrt{\sum_{i=1}^{N_{\text{ТМП}}^{(q)}} \left(\partial y / \partial x_i\, \sigma(x_i) \right)^2}\,,$$

где $y_q(x)$, $q = \overline{1, N_{\text{ЛТХ}}}$ – ЛТХ, используемая в СПО мониторинга. ЛТХ приведены в технической документации; $y_q = f(x_i)$, $i = \overline{1, N_{\text{ТМП}}^{(q)}}$ – функция q-й ЛТХ от ТМП x_i, приводится в технической документации; $\sigma(y_q)$ – СКО приведенной погрешности вычисления q-й ЛТХ; $\sigma(x_i)$ – СКО приведенной погрешности измерения i-го датчика.

Показатель p_2 характеризует погрешность оценок ЛТХ, формируемую вычислительными процедурами над телеизмерениями. Принимается допущение о нормальном распределении погрешности.

Частный показатель p_3 – своевременность получения результата мониторинга – вычисляется по формуле

$$p_3 = \frac{1}{\dfrac{\left| T_{\text{тр}} - T_{\text{Ш}} \right|}{T_{\text{тр}}} + 1}\,,$$

где $T_{\text{Ш}}$ – длительность подготовки исходной информации и применения СПО для мониторинга процесса функционирования ПГС от команды «Продувка» до окончания работы ДУШ; $T_{\text{тр}} = 3$ ч – длительность оперативной и экспресс-обработки и анализа ТМИ согласно [10].

При вычислении значения показателя p_3 используется время окончания формирования прогнозируемой траектории процесса, включающего максимальное количество операций. Данный показатель характеризует соответствие временно́го интервала подготовки исходной информации и применения СПО мониторинга отведенному интервалу оперативной и экспресс-обработки и анализа ТМИ.

Частный показатель p_4 – оперативность получения результата мониторинга – вычисляется по формуле

$$p_4 = \frac{1}{\dfrac{T_{\text{П}}}{T_{\text{тр}}} + 1}\,,$$

где $T_{\text{П}}$ – длительность подготовки исходной информации и применения СПО для мониторинга процесса подготовки носителя к пуску – от команды «Продувка» до команды «Пуск», когда возможно формирование команды на аварийное выключение двигателя (АВД) без потери полезной нагрузки (ПН).

При вычислении значения показателя p_4 используется время окончания формирования прогнозируемой траектории процесса, включающего минимальное количество операций. Показатель характеризует быстроту получения минимально необходимого результата мониторинга.

Частный показатель p_5 – полнота обрабатываемой измерительной информации – вычисляется по формуле

$$p_5 = \frac{N_{\text{ТМП}}}{N_{\text{ТМП}}^{\text{ДПМ}}}\,,$$

где $N_{\text{ТМП}}$ – количество ТМП, используемых в СПО мониторинга; $N_{\text{ТМП}}^{\text{ДПМ}} = 59$ ед. – количество ТМП, телеметрирующих процессы в ПГС согласно программе телеизмерений.

Показатель характеризует степень использования доступной измерительной информации по ПГС в СПО мониторинга.

Частный показатель p_6 – полнота вычисляемых ЛТХ – рассчитывается по формуле

$$p_6 = \frac{N_{\text{ЛТХ}}}{N_{\text{ЛТХ}}^{\text{ИЭ20}}}\,,$$

где $N_{\text{ЛТХ}}$ – количество ЛТХ, оценки которых используются в СПО мониторинга; $N_{\text{ЛТХ}}^{\text{ИЭ20}} = 109$ ед. – количество ЛТХ, характеризующих ПГС ДУ РН «Союз-2», в соответствии с технической документацией.

Показатель определяет соотношение используемых в процессе мониторинга ЛТХ к общему количеству контрольных параметров, характеризующих ПГС.

Частный показатель p_7 – полнота учитываемых нештатных ситуаций – рассчитывается по формуле

$$p_7 = \frac{N_{\text{АВД}}}{N_{\text{АВД}}^{\text{ТО}}}\,,$$

где $N_{\text{АВД}}$ – количество учитываемых нештатных ситуаций в СПО мониторинга; $N_{\text{АВД}}^{\text{ТО}} = 25$ ед. – количество нештатных

ситуаций, приводящих к прекращению подготовки носителя к пуску и к АВД при работе ДУ, приведенных в технической документации.

Показатель характеризует глубину учитываемых нештатных ситуаций, предусмотренных в технической документации.

Частный показатель p_8 – полнота моделируемого технологического процесса – рассчитывается по формуле

$$p_8 = \frac{N_{\text{МОН}}}{N_{\text{ТО}}},$$

где $N_{\text{МОН}}$ – количество моделируемых в СПО мониторинга операций процесса функционирования ПГС ДУ; $N_{\text{ТО}} = 176$ ед. – количество операций, предусмотренных в технической документации.

Показатель характеризует адекватность модели процесса функционирования ПГС ДУ своему прототипу.

Частный показатель p_9 – анализируемость синтезированной модели процесса с учетом реализации различных видов ограничений процесса – рассчитывается по формуле

$$p_9 = \frac{N_{\text{ОГР}}}{N_{\text{ПОГ}}},$$

где $N_{\text{ОГР}}$ – виды ограничений, реализуемые в СПО мониторинга: для СЛП – ресурсные, временные, технические и технологические; для рекурсивной модели – временные; $N_{\text{ПОГ}} = 5$ ед. – виды ограничений, потенциально применяемые при мониторинге процессов ПГС ДУ РН «Союз-2»; дополнительно к указанным – функциональные.

Показатель характеризует способность СПО реализовывать собственными средствами различные типы ограничений процесса, мониторинг которого осуществляется.

Частный показатель p_{10} – верифицируемость синтезированной модели процесса – рассчитывается по формуле

$$p_{10} = \frac{N_{\text{ОШ}}}{N_{\text{ПО}}},$$

где $N_{\text{ОШ}}$ – количество типов ошибок, выявляемых и корректируемых СПО мониторинга: для СЛП – непротиворечивость ресурсных ограничений, корректность по входу и выходу операций, активность операций; для рекурсивной модели – активность операций; $N_{\text{ПО}} = 5$ ед. – количество типов ошибок, потенциально формируемых при синтезе модели технологического процесса в предметной области; дополнительно к предыдущим – достижимость требуемого состояния процесса.

Показатель характеризует способность СПО к автоматическому поиску ошибок в модели процесса функционирования ПГС ДУ.

Частный показатель p_{11} – однозначность результата мониторинга при неизменности измерительной информации – рассчитывается по формуле

$$p_{11} = \frac{N_{\text{УТМП}}}{N_{\text{ТОП}}},$$

где $N_{\text{УТМП}}$ – количество учитываемых в СПО мониторинга операций, свойства которых определяются результатами контроля ТМП; $N_{\text{ТОП}} = 113$ ед. – полное количество операций, свойства которых определяются результатами контроля ТМП.

Показатель характеризует степень влияния, не учитываемого в СПО измерительной информации, на результат мониторинга технологического процесса.

Частный показатель p_{12} – редактируемость синтезированной модели процесса – рассчитывается по формуле

$$p_{12} = \frac{N_{\text{РЕД}}}{N_{\text{ПР}}},$$

где $N_{\text{РЕД}}$ – количество вариантов изменения траектории, реализуемых СПО мониторинга: для СЛП – автоматизированное (ручное и автоматическое) изменение типа меток отсчета состояния, начало, остановка, приостановка, возобновление операции; для рекурсивной модели – ручное начало, остановка, приостановка и возобновление операции; $N_{\text{ПР}} = 10$ ед. – количество вариантов изменения траектории процесса, потенциально реализуемых при синтезе модели процесса в предметной области.

Показатель p_{12} характеризует реализуемость возможных вариантов изменения траектории синтезированной модели процесса средствами СПО-мониторинга.

Частный показатель p_{13} – повторяемость синтезированной модели процесса общесистемным ПО – рассчитывается по формуле

$$p_{13} = \frac{N_{\text{ПВ}}}{N_{\text{МОН}}},$$

где $N_{\text{ПВ}}$ – количество операций, имеющих временные ограничения. Реализация данных ограничений возможна средствами MicrosoftProject.

Таким образом, предложено 13 частных показателей. Они, несомненно, специализированы, благодаря этому можно оценить качество СПО мониторинга функционирования ПГС ДУ РН «Союз-2». Такая оценка будет объективна (все показатели количественные), полна (рассматриваются эксплуатационные показатели, показатели сопровождения СПО и результативности мониторинга) и показательна (оценки показателей для различных реализаций СПО значимо разделяются).

Полиномиальный подход к комплексированию показателей

Для комплексирования частных показателей качества мониторинга технологического процесса использовался подход с применением нечеткой логики и положений теории планирования эксперимента, который получил широкую известность под названием полиномиального подхода [15–17]. Этот подход выгодно отличается легкостью применения, доступной трактовкой результатов, а главное – формированием оценок важности не только отдельных частных показателей, но и их сочетаний.

Полиномиальный подход заключается в выполнении следующих шагов:

1) формирование множества частных показателей качества функционирования некоторого сложного технического объекта;

2) нормирование шкал частных показателей к интервалу $[-1;1]$;

3) формирование лингвистической переменной, понимаемой экспертом как искомый интегральный показатель в вербальном представлении;

4) формирование достаточного (по внутреннему убеждению эксперта) множества возможных значений лингвистической переменной – термов, например: низкое, среднее и высокое значения, или низкое, ниже среднего, среднее, выше среднего и высокое значения;

5) дефаззификация значений лингвистической переменной, т. е. сопоставление экспертом в соответствии с внутренними убеждениями каждому значению лингвистической переменной вещественного числа из интервале от 0 до 1. Таким образом эксперт формирует требуемые значения интегрального показателя для всех вариантов сочетаний крайних значений частных показателей;

6) формирование плана опроса эксперта о значении лингвистической переменной для всех вариантов сочетаний крайних значений частных показателей;

7) формирование ортогонального плана экспертного опроса. Ортогональный план строится на основе данных бланка экспертного опроса путем добавления пар, троек и т. д. частных показателей, а также дополнительного элемента, не содержащего частных показателей. Крайние значения пар, троек и т. д. частных показателей вычисляются по правилу логического умножения значений составляющих частных показателей;

8) расчет коэффициентов интегрального полинома;

9) формирование интегрального полинома для вычисления искомого интегрального показателя.

Анализ количества частных показателей качества мониторинга функционирования ПГС позволяет сделать вывод о практически нереализуемой мощности требуемого в соответствии с полиномиальным подходом бланка экспертного опроса. Необходимо задать эксперту $2^{13} = 8192$ вопроса с вариантами сочетаний крайних значений частных показателей. В таком случае рекомендуется осуществлять комплексирование частных показателей на подгруппы мощностью не более четырех элементов. При этом необходимо обязательно соблюсти физическую однородность комплексируемых в одну группу показателей.

Схема комплексирования частных показателей качества мониторинга приведена на рис. 1.

С учетом принципиального различия целей процесса мониторинга на разных этапах жизненного цикла РН «Союз-2» задача расчета ЕКИП применялась для следующих случаев:

1) РМВ (режим реального времени) – мониторинг функционирования ПГС ДУ РН «Союз-2» на этапе оперативной и экспресс-обработки и анализа ТМИ. Это участки подготовки, пуска РН и активный участок траектории, временно́й интервал формирования общих выводов о результатах испытаний и применения РН (до 3 ч после пуска, согласно [10]);

2) ППО (послеполетная обработка) – анализ функционирования систем ПГС ДУ РН «Союз-2» на этапе послеполетной обработки ТМИ. Это временной интервал до 30 суток после пуска, в течение которого формируется оперативный отчет по результатам подготовки к пуску, пуска и полета изделия, согласно [10];

3) ПНИ (подготовка новых изделий) – подготовка СПО, подготовка спецификации процесса, создание и верификация моделей для вновь вводимых изделий РКТ или при модифицировании систем в существующих типах РКТ. Это временной интервал до 3–4 месяцев перед планируемым пуском новой (модифицированной) РН;

4) ПОГ (пополнение орбитальной группировки) – мониторинг функционирования ПГС РН «Союз-2» на этапе оперативного пополнения орбитальной группировки космических аппаратов (КА).

Комплексированные показатели качества мониторинга функционирования ПГС РН «Союз-2»

На основе перечня частных показателей, схемы их комплексирования (рис. 1) и различных случаев применения СПО мониторинга (см. предыдущий пункт) необходимо сформировать интегральные полиномы для вычисления интегрального показателя качества:

– существующего СПО-мониторинга,

– СПО, разработанного на основе СЛП,

– СПО с требуемым качеством.

Для лингвистической переменной сформированы значения: «очень низкое (ОН)», «низкое (Н)», «ниже среднего (НС)», «среднее (С)», «выше среднего (ВС)», «высокое (В)» и «очень высокое (ОВ)». Дефаззификация проведена следующим образом: ОН – 0; Н – 0,1; НС – 0,3; С – 0,5; ВС – 0,7; В – 0,9; ОВ – 1.

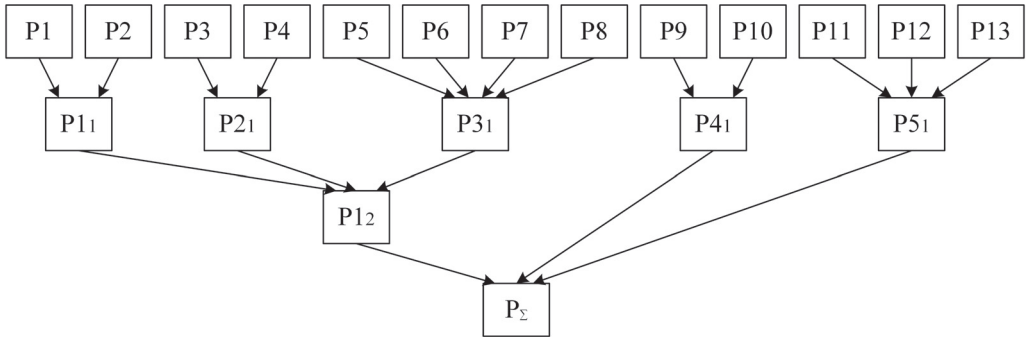


Рис. 1. Схема комплексирования частных показателей.

$P1$–$P13$ – рассмотренные частные показатели качества; $P1_1$ – комплексированный показатель степени доверия к результатам мониторинга; $P2_1$ – комплексированный показатель степени соответствия временно́й характеристики результата мониторинга требуемому значению; $P3_1$ – комплексированный показатель степени адекватности синтезированной для мониторинга модели технологического процесса своему прототипу; $P4_1$ – комплексированный показатель диагностируемости модели технологического процесса, характеризующий степень пригодности модели для поиска ошибок и недостатков; $P5_1$ – комплексированный показатель модифицируемости модели технологического процесса, характеризующий степень пригодности модели для совершенствования; $P1_2$ – комплексированный показатель эксплуатационных характеристик применения СПО-мониторинга; P_Σ – единый конечный интегральный показатель (ЕКИП) качества мониторинга технологического процесса

В табл. 1 приведен пример бланка экспертного опроса для комплексированного показателя $P1_1$. Бланки для расчета показателей $P1_2, P4_1$ и $P5_1$ имеют аналогичное представление и здесь не приводятся.

Результаты расчета коэффициентов интегрального полинома для разных случаев приведены в табл. 2.

Таблица 1

Бланк экспертного опроса о показателе $P1_1$

№ п/п	Крайние значения частных показателей		Значение лингвистической переменной			
	p_1	p_2	РМВ	ППО	ПНИ	ПОГ
1	–1	–1	ОН	ОН	ОН	ОН
2	–1	1	В	В	В	В
3	1	–1	НС	НС	Н	НС
4	1	1	ОВ	ОВ	ОВ	ОВ

Таблица 2

Коэффициенты интегрального полинома для разных случаев

Коэффициент	Значение коэффициента интегрального полинома для режима применения СПО мониторинга			
	РМВ	ППО	ПНИ	ПОГ
λ_0	0,46	0,45	0,50	0,60
λ_1	0,21	0,13	0,13	0,30
λ_2	0,11	0,18	0,18	0,20
λ_3	0,09	0,13	0,18	0,00
λ_4	–0,14	0,00	0,05	–0,14
λ_5	0,09	0,05	0,05	0,05
λ_6	0,09	0,00	–0,10	–0,05
λ_7	0,09	0,08	0,03	0,00

Полином для каждого случая примет вид

$$P = \lambda_0 + \lambda_1 P1_2 + \lambda_2 P4_1 + \lambda_3 P5_1 + \lambda_4 P1_2 P4_1 + \\ + \lambda_5 P1_2 P5_1 + \lambda_6 P4_1 P5_1 + \lambda_7 P1_2 P4_1 P5_1.$$

Результаты расчета для разных случаев применения СПО-мониторинга представлены на рис. 2.

Для наглядности используются только коэффициенты, характеризующие индивидуальную важность показателей $P1_2, P4_1$ и $P5_1$. Это коэффициенты, соответственно, λ_1, λ_2 и λ_3. Коэффициенты, характеризующие совместную важность показателей, не учтены. На рис. 2 по осям отложены значения комплексированных показателей эксплуатационных характеристик ($P1_2$) СПО-мониторинга, диагностируемости ($P4_1$) и модифицируемости ($P5_1$) синтезированной модели с помощью СПО-мониторинга. Кроме того, на рис. 2:

– сплошной линией соединены значения комплексируемых показателей для случая ПОГ;

– штриховой линией с коротким шагом – ПНИ;

– штриховой линией с длинным шагом – РМВ;

– пунктирной линией – ППО.

Анализ рис. 2 позволяет сделать следующие выводы.

Эксплуатационные характеристики ($P1_2$) включают показатели достоверности, оперативности и адекватности модели функционирования ПГС ДУ РН «Союз-2». Такие характеристики наиболее важны в случае мониторинга в реальном времени при подготовке, пуске и полете РН и при оперативном пополнении орбитальной группировки КА, т. е.

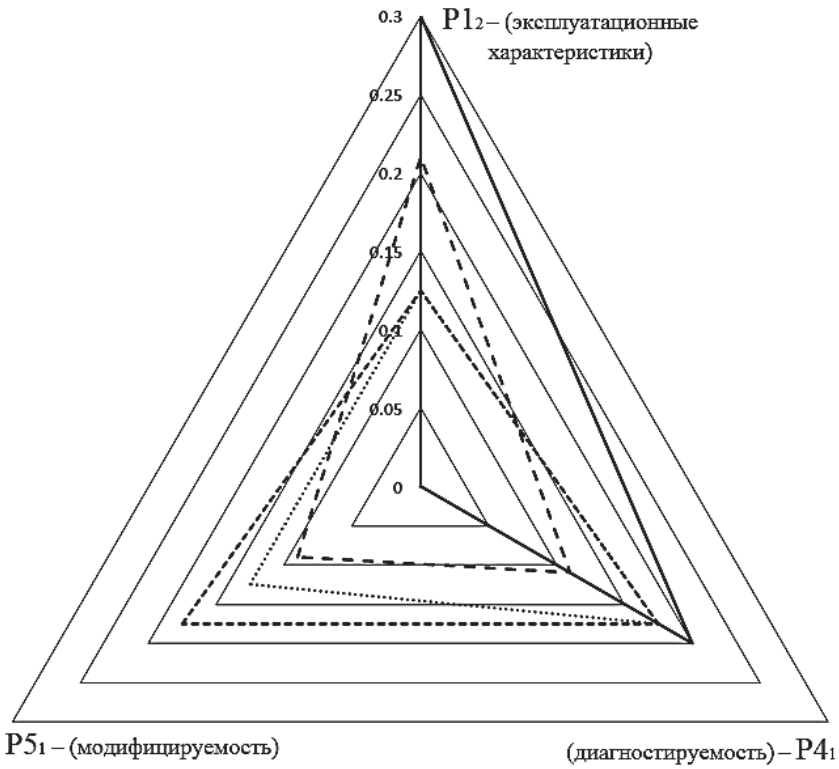


Рис. 2. Предпочтения экспертной группы при определении важности показателей в разных случаях применения СПО-мониторинга

в случаях, когда наиболее важно максимально быстро и точно принять решение о техническом состоянии носителя и прогнозировать успешность выполнения им своей целевой задачи.

Показатели диагностируемости ($P4_1$) модели функционирования ПГС характеризуют степень пригодности модели для поиска ошибок и недостатков в технологическом процессе. Такие показатели имеют примерно одинаковую важность во всех случаях. Причиной данного факта является чрезвычайно большая стоимость ошибки в прогнозе развития технологического процесса в рассматриваемой предметной области.

Показатели модифицируемости ($P5_1$) модели функционирования ПГС характеризуют степень пригодности модели для модификации и совершенствования. Такие показатели наиболее важны в случае подготовки к мониторингу вновь вводимых изделий РКТ. В таком случае наиболее важна возможность оперативной глубокой перенастройки модели технологического процесса под изменяющиеся, неустоявшиеся и неточные характеристики внедряемой техники.

Таким образом, сформирован порядок оценивания качества мониторинга технологического процесса функционирования ПГС ДУ РН «Союз-2» в разных случаях применения СПО. Теперь необходимо сформировать порядок расчета ЕКИП качества мониторинга. Формально необходимо комплексировать показатели $P1_2$, $P4_1$ и $P5_1$ качества мониторинга в разных случаях в ЕКИП качества P_Σ.

Множеством частных показателей в этом случае будет множество

$$P_\Sigma = \{p_{\text{РМВ}},\ p_{\text{ППО}},\ p_{\text{ПНИ}},\ p_{\text{ПОГ}}\}.$$

Все элементы множества P_Σ вычисляются с помощью соответствующих интегральных полиномов, коэффициенты которых приведены в табл. 2. Исходная шкала значений всех показателей включает интервал $[0;1]$.

Используем лингвистическую переменную «Качество мониторинга функционирования ПГС ДУ РН „Союз-2“ с применением СПО на основе…» со значениями, аналогичными ранее введенной переменной, и с аналогичным порядком дефаззификации этих значений.

Результаты расчета коэффициентов интегрального полинома для ЕКИП P_Σ приведены в табл. 3.

Таблица 3

Коэффициенты интегрального полинома для ЕКИП P_Σ

№ коэффициента	Значение коэффициента	№ коэффициента	Значение коэффициента
0	0,69	8	–0,03
1	0,01	9	–0,04
2	0,10	10	–0,05
3	0,04	11	0,00
4	0,23	12	0,04
5	0,00	13	0,03
6	–0,06	14	0,06
7	–0,03	15	0,01

В данной таблице номера коэффициентов обозначают номера коэффициентов λ_0 –λ_{15}. Полином для ЕКИП P_Σ примет вид

$$P_\Sigma = \lambda_0 + \lambda_1 P_{\text{РМВ}} + \lambda_2 P_{\text{ППО}} + \lambda_3 P_{\text{ПНИ}} + \lambda_4 P_{\text{ПОГ}} + \lambda_5 P_{\text{РМВ}} P_{\text{ППО}} + \lambda_6 P_{\text{РМВ}} P_{\text{ПНИ}} + \lambda_7 P_{\text{РМВ}} P_{\text{ПОГ}} + \lambda_8 P_{\text{ППО}} P_{\text{ПНИ}} + \lambda_9 P_{\text{ППО}} P_{\text{ПОГ}} + \lambda_{10} P_{\text{ПНИ}} P_{\text{ПОГ}} + \lambda_{11} P_{\text{РМВ}} P_{\text{ППО}} P_{\text{ПНИ}} + \lambda_{12} P_{\text{РМВ}} P_{\text{ППО}} P_{\text{ПОГ}} + \lambda_{13} P_{\text{РМВ}} P_{\text{ПНИ}} P_{\text{ПОГ}} + \lambda_{14} P_{\text{ППО}} P_{\text{ПНИ}} P_{\text{ПОГ}} + \lambda_{15} P_{\text{РМВ}} P_{\text{ППО}} P_{\text{ПНИ}} P_{\text{ПОГ}}.$$

При анализе табл. 3, а именно λ_1–λ_4 следует отметить, что для инженера-испытателя Информационно-аналитического центра космодрома значительно преобладающим по важности случаем функционирования СПО-мониторинга является ПОГ (λ_4). Действительно, значимость быстрого и достоверного получения результата мониторинга при пополнении орбитальной группировки – необходимое условие успешного выполнения космодромом задачи по предназначению.

Следующим по важности случаем является ППО (λ_2) – послеполетная обработка и анализ информации, так как требуется максимально достоверно и своевременно подготовить заключение в оперативный отчет о причинах нештатных ситуаций, аварий и катастроф (при их наличии).

ПНИ (λ_3) – следующий (третий) по важности случай. Значимость СПО-мониторинга заключается в предоставлении специалисту-пользователю инструмента для быстрого формирования моделей рассматриваемых технологических процессов. Цель применения такого СПО – быстрое построение и освоение новых технологических процессов.

Минимальным по важности остается РМВ (λ_1) – обработка и анализ ТМИ в период подготовки к пуску, пуска и активного участка траектории полета РН, а также оперативной и экспресс-обработки и анализа ТМИ. Данный факт объясняется низкими возможностями управления технологическими процессами на данном временно́м интервале. Здесь основная задача мониторинга функционирования ПГС ДУ РН «Союз-2» – оперативно подготовить заключение о функционировании систем и агрегатов РН в доклад старшему начальнику по результатам пуска.

Таким образом, полностью рассмотрен порядок вычисления структуры интегрального полинома, позволяющего по заданным характеристикам СПО мониторинга вычислить ЕКИП качества мониторинга функционирования ПГС ДУ РН «Союз-2».

Интегральный показатель качества мониторинга функционирования ПГС РН «Союз-2»

Для вычисления значения ЕКИП качества мониторинга функционирования ПГС ДУ РН «Союз-2» был проведен подробный анализ практической реализации на космодроме варианта информационного обеспечения автоматизированной системы управления испытаний и применения РКТ. В частности, рассматривалось информационное обеспечение в приложении мониторинга технологических процессов подготовки и пуска РН «Союз-2», оперативной, экспресс- и послеполетной обработки и анализа измерительной информации. По указанным показателям было оценено существующее СПО.

Кроме того, путем анализа документов [10–12] и технической документации были сформированы требуемые

значения частных показателей. Требуемые значения показателей 1–4 получены в точном виде, остальных показателей – путем обработки экспертных высказываний. Достоверность экспертных высказываний о требуемых значениях этих показателей достигается широким охватом экспертов. Обоснованность достигается предъявлением одновременно с формулировкой запроса вычисленного значения частного показателя для используемого применяемого СПО и для разработанного СПО. Тем самым задача эксперта облегчается, так как он имеет числовые точки отсчета, относительно которых высказывает свое мнение о желаемом (требуемом) качестве СПО мониторинга.

Результаты оценивания частных показателей приведены в табл. 4. Все показатели находятся в исходной шкале [0;1].

Таблица 4

Значения частных показателей качества мониторинга ПГС (в исходной шкале)

Частный показатель	Существующее СПО на основе рекурсивной модели	Требуемое значение	СПО на основе СЛП
p_1	0,94	0,90	0,81
p_2	0,89	0,85	0,75
p_3	0,33	0,90	0,92
p_4	0,26	0,80	0,96
p_5	0,14	0,75	0,83
p_6	0,07	0,75	0,8
p_7	0,03	0,75	0,88
p_8	0,55	0,75	0,92
p_9	0,20	0,75	0,80
p_{10}	0,20	0,75	0,80
p_{11}	0,21	0,75	0,97
p_{12}	0,40	0,75	1,00
p_{13}	0,87	0,75	0,45

Анализ табл. 4 позволяет сделать вывод, что внедряемое СПО не достигло требуемого значения по частным показателям p_1, p_2 и p_{13}.

Причиной данного факта относительно частных показателей p_1 и p_2 является большое количество ТМП и ЛТХ при мониторинге, вследствие чего возрастает погрешность используемой информации. Однако это плата за значительное повышение остальных частных показателей.

Причиной недостижения требуемого значения по частному показателю p_{13} является функциональная ограниченность общесистемного ПО, не приспособленного для решения специальных задач, возникающих при мониторинге технологических процессов функционирования РКТ.

Результаты оценивания комплексированных показателей для различных режимов приведены в табл. 5. Также в таблице приведено значение ЕКИП качества СПО мониторинга: для существующего варианта исполнения, варианта исполнения на основе СЛП и для варианта исполнения, при котором все показатели равняются требуемым значениям. Все показатели находятся в исходной шкале [0;1].

Анализ табл. 5 позволяет сделать следующие выводы.

Существующее СПО мониторинга, функционирующее на космодроме, входящее в информационное обеспечение автоматизированной системы управления испытаний и применения РКТ, не удовлетворяет специалистов-пользователей ни на одном временно́м интервале применения СПО мониторинга. Как следствие, нас не удовлетворяет и ЕКИП качества существующего СПО мониторинга. Это является практической проблемой, вызвавшей необходимость создания СЛП.

Таблица 5

Итоговые оценки показателя качества мониторинга функционирования ПГС ДУ РН «Союз-2»

Режим	Оцениваемые варианты СПО мониторинга		
	Существующее СПО мониторинга	Требуемое значение показателя	Разработанное СПО на основе СЛП
РМВ	0,42	0,71	0,69
ППО	0,42	0,77	0,81
ПНИ	0,40	0,77	0,84
ПОГ	0,48	0,88	0,92
ЕКИП P_Σ	0,65	0,90	0,92

Приведенные в табл. 5 значения ЕКИП позволяют сделать вывод, что СПО на основе СЛП по качеству превышает существующее на 27%, а требования – на 2%. Это доказывает оправданность разработки и внедрения нового СПО.

Заключение

В работах [5, 6] предложен оригинальный подход к мониторингу технологических процессов в предметной области функционирования РКТ, а также обработки и анализа ее измерительной информации. На основе СЛП разработано СПО, выполняющее задачу мониторинга функционирования ПГС ДУ РН «Союз-2».

Материал посвящен разработке специализированной системы показателей качества СПО мониторинга технологических процессов в предметной области. В системе используется 13 количественных показателей нижнего уровня. Данные показатели комплексируются в 6 показателей верхних уровней. Последние в свою очередь формируют ЕКИП качества СПО мониторинга. При комплексировании использовался известный полиномиальный подход.

По разработанной системе показателей были оценены применяемое в Информационно-аналитическом центре космодрома СПО, а также СПО на основе разработанного автором СЛП. Кроме того, по системе показателей были сформированы требуемые значения показателей. Расчет показателей позволяет сделать вывод, что качество внедряемого СПО значительно превышает существующее и удовлетворяет требуемым значениям.

Разработанную систему показателей качества рекомендуется использовать при оценивании качества СПО в предметной области обработки и анализа ТМИ РКТ. С помощью модификации системы показателей можно ее адаптировать для достаточно широкого круга СПО.

Литература

1. Бураков В. В. Управление качеством программных средств: моногр. / В. В. Бураков. – СПб.: ГУАП, 2009. – 288 с.

2. Fenton N. E. Software Metrics: Roadmap / N. E. Fenton, M. Neil // ICSE '00 Proc. Conf. The Future of Software Eng., 2000. P. 357–370.

3. Boehm B. W. Software Engineering Economics / B. W. Boehm. – New Jersey: Prentice-Hall. Inc., Englewood Cliffs, 1981. – 767 p.

4. Goodman P. P. Software Metrics: Best Practices for Successful IT Management / P. P. Goodman. – Rothstein Associates, 2004. – 264 p.

5. Шмелев В. В. Модели технологических процессов функционирования космических средств / В. В. Шмелев // Авиакосмическое приборостроение. – 2015. – № 4. – С. 78–93.

6. Шмелев В. В. Сравнительный анализ структурно-логического подхода к моделированию технологических процессов функционирования ракетно-космической техники / В. В. Шмелев, М. Ю. Охтилев // Информационно-управляющие системы. – 2016. – № 5 (84). – С. 35–44.

7. Лескин А. А. Сети Петри в моделировании и управлении / А. А. Лескин, П. А. Мальцев, А. М. Спиридонов. – Л.: Наука, 1989. – 133 с.

8. ГОСТ Р ИСО/МЭК 25021-2014. Информационные технологии. Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения. (SQuaRE). Элементы показателя качества. – М.: Стандартинформ, 2015. – 103 с.

9. ГОСТ Р ИСО/МЭК 25010-2015. Информационные технологии. Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения (SQuaRE). Модели качества систем и программных продуктов. – М.: Стандартинформ, 2016. – 36 с.

10. ГОСТ 1410-002-2010. Ракетно-космическая техника. Система информации о техническом состоянии и надежности космических комплексов и входящих в их состав изделий. Основные положения. – М.: Стандартинформ, 2011. – 49 с.

11. Шмелев В. В. Систематизация требований к разработке перспективных аппаратно-программных комплексов обработки телеметрической информации ракетно-космической техники / В. В. Шмелев, В. В. Ткаченко // Тр. Военно-космич. акад. им. А. Ф. Можайского. – 2015. – С. 38–46.

12. Куренков В. И. Конструкция и проектирование изделий ракетно-космической техники. Ч. 2. Основы проектирования ракет-носителей / В. И. Куренков. – Самара: Самар. гос. аэрокосмич. ун-т им. С. П. Королева (нац. исслед. ун-т), 2012. – 304 с.

13. Шмелев В. В. Моделирование процесса послеполетного анализа телеметрической информации по результатам подготовки, пуска и полета ракеты-носителя «Союз-2» / В. В. Шмелев // Оборонный комплекс – научно-техническому прогрессу России. – 2016. – № 1. – С. 36–48.

14. http://npoit.ru/products/item/high/abc-059 (дата обращения 09.02.2017).

15. Спесивцев А. В. Управление рисками чрезвычайных ситуаций на основе формализации экспертной информации / А. В. Спесивцев. – СПб.: Изд-во Политехнич. ун-та, 2004. – 238 с.

16. Зеленцов В. А. Многокритериальный анализ влияния отдельных элементов на работоспособность сложной системы / В. А. Зеленцов, А. Н. Павлов // Информационно-управляющие системы. – 2010. – № 6 (49). – С. 7–12.

17. Павлов А. Н. Модели и методы планирования реконфигурации сложных объектов с перестраиваемой структурой: дис. ... д-ра техн. наук. – СПб., 2014. – 381 с.

Indicators of Quality Monitoring System Processes in the Aerospace Industry

Shmelev V. V.
A. F. Mozhaisky Military Space Academy
St. Petersburg, Russia
valja1978@yandex.ru

Annotation. **The article offers a specialized four-level system of quality indicators for the integrated evaluation of monitoring the functioning of the fluid system of the carrier rocket Soyuz-2. System 13 comprises a lower performance level and the upper level 6 of indicators. In contrast to existing analogs and recommendations of all the indicators in the quantitative system. This objective assessment is achieved. Completeness assessment provided by the inclusion in the system of indicators and operational and maintenance performance, and effectiveness. In the described system is estimated quality monitoring using software options based on a recursive model and the structural and logical approach, as well as forming the required values of parameters satisfying the experts.**

Keywords: **software quality, rocket and space technology, someone pleksirovanie private indicators, process monitoring, structural and logical approach, recursive process model, process modeling.**

References

1. Burakov V. V. *Upravleniekachestvom programmnyh sredstv* [Management Software Quality], St. Petersburg, GUAP, 2009, 288 p.

2. Fenton N. E., Neil M. Software Metrics: Roadmap, *ICSE '00 Proc. Conf. The Future of Software Eng*., 2000, pp. 357-370.

3. Barry W. Boehm. Software Engineering Economics. Prentice-Hall. New Jersey, Inc., Englewood Cliffs, 1981, 767 p.

4. Goodman P. P. Software Metrics: Best Practices for Successful IT Management. Rothstein Associates, 2004. 264 p.

5. Shmelev V. V. Models of Processes of Functioning of Space Assets [Modeli tekhnologicheskih processov funkcionirovaniya kosmicheskih sredstv], *Aviakosmicheskoe priborostroenie [Aerospace Instrument]*, 2015, no. 4, pp. 78-93.

6. Shmelev V. V., Ohtilev M. Yu. Comparative Analysis of Structural and Logical Approach to the Modeling of Processes of Functioning of Rocket and Space Technology [Sravnitel'nyj analiz strukturno-logicheskogo podhoda k modelirovaniyu tekhnologicheskih processov funkcionirovaniya raketno-kosmicheskoj tekhniki], *Informacionno-upravlyayushchie sistemy [Information and Control Systems]*, 2016, no. 5 (84), pp. 35-44.

7. Leskin A. A., Mal'cev P. A., Spiridonov A. M. *Seti Petri v modelirovaniiiupravlenii* [Petri Nets in Modeling and Management], Leningrad, Nauka, 1989, 133 p.

8. GOST R ISO 25021-2014. Information Technology. System and Software Engineering. Requirements and Assessment of Quality Systems and Software. (SQuaRE). Elements of Quality Score [Informacionnye tekhnologii. Sistemnaya i programmnaya inzheneriya. Trebovaniya i ocenka kachestva sistem i programmnogo obespecheniya. (SQuaRE). Ehlementy pokazatelya kachestva], Moscow, 2015, 103 p.

9. GOST R ISO 25010-2015. Information Technology. System and Software Engineering. Requirements and Assessment of Quality Systems and Software (SQuaRE). Models of Quality Systems and Software Products [Informacionnye tekhnologii. Sistemnaya i programmnaya inzheneriya. Trebovaniya i ocenka kachestva sistem i programmnogo obespecheniya (SQuaRE). Modeli kachestva sistem i programmnyh produktov], Moscow, 2016, 36 p.

10. GOST 1410-002-2010. Rocket and Space Equipment. System Information About the Technical Condition and Reliability of Space Systems and Their Constituent Products. The Main Provisions [Raketno-kosmicheskaya tekhnika. Sistema informacii o tekhnicheskom sostoyanii i nadezhnosti kosmicheskih kompleksov i vhodyashchih v ih sostav izdelij. Osnovnye polozheniya], Moscow, 2011, 49 p.

11. Shmelev V. V., TkachenkoV. V. Ordering of Requirements for the Development of Advanced Hardware and Software of Telemetry Data Processing Systems of Rocket and Space Technology [Sistematizaciya trebovanij k razrabotke perspektivnyh apparatno-programmnyh kompleksov obrabotki telemetricheskoj informacii raketno-kosmicheskoj tekhniki], *Trudy Voenno-kosmicheskoj akademii imeni A. F. Mozhajskogo [Proc. Military Space Acad. named after A. F. Mozhaiskogo]*, 2015, pp. 38-46.

12. Kurenkov V. I. *Konstrukciya i proektirovanie izdelij raketno-kosmicheskoj tekhniki. CHast' 2. Osnovy proektirovaniya raket-nositelej* [Design and Engineering Space Engineering. Part 2: Fundamentals of Rockets], Samara, Samarskiy gosudarstvenniy aehrokosmicheskiy universitet imeni S. P. Koroleva, 2012, 304 p.

13. Shmelev V. V. Simulation of The Process of Post-Flight Analysis of Telemetry Data on the Preparation, Launch and Flight of the Carrier Rocket Soyuz-2 [Modelirovanie processa poslepoletnogo analiza telemetricheskoj informacii po rezul'tatam podgotovki, puska i poleta rakety-nositelya Soyuz-2], *Oboronnyj kompleks – nauchno-tekhnicheskomu progressu Rossii [Defensive Complex – Scientific and Technical Progress of Russia]*, 2016, no. 1, pp. 36-48.

14. http://npoit.ru/products/item/high/abc-059 (accessed 9 February 2017).

15. Spesivcev A. V. *Upravlenie riskami chrezvychajnyh situacij na osnove formalizacii ehkspertnoj informacii* [Emergency Risk Management Based on Formalization of Expert Information], St. Petersburg, Politekhnicheskiy universitet, 2004, 238 p.

16. Zelencov V. A., Pavlov A. N. Multi-criteria Analysis of the Impact of Individual Elements on the Performance of a Complex System [Mnogokriterial'nyj analiz vliyaniya otdel'nyh ehlementov na rabotosposobnost' slozhnoj sistemy], *Informacionno-upravlyayushchie sistemy [Information and Control Systems]*, 2010, no. 6 (49), pp.7-12.

17. Pavlov A. N. Models and Methods of Planning Reconfiguration of Complex Objects with Reconfigurable Structure [Modeli i metody planirovaniya rekonfiguracii slozhnyh ob"ektov s perestraivaemoj strukturoj], St. Petersburg, 2014, 381 p.

Approach to Internet of Things Detection of Security Incidents Using SIEM Technology

Zegzhda D. P., Lavrova D. S.
Peter the Great St. Petersburg Polytechnic University
St. Petersburg, Russia
dmitry.zegzhda@ibks.ftk.spbstu.ru, lavrova@ibks.spbstu.ru

Abstract. **In this article authors propose an approach to detection of security incidents in Internet of things using SIEM technology. Proposed approach takes into account such Internet of things characteristics as high heterogeneity of devices and large number of implicit logical connections between devices during technological processes implementation. Also it is formalized the "security event" notion for Internet of things based on graph model.**

Keywords: **Internet of Things, security incident, SIEM, security analysis, data aggregation, ontology.**

Introduction

Internet of things (IoT) concept involves the association of physical objects in networks using built-in technologies, so that these objects get an ability to interact with each other and with the outside world, without human interaction [1]. Internet of Things integration with all spheres of human activity has led to emergence of large-scale complex IoT systems, which include a wide variety of devices. Successful attacks implementation on IoT system is capable to cause harm to human life, and therefore the problem of providing security in IoT is extremely important.

SIEM (security information and event management) technology is a prospective technology for providing security in large-scale systems. SIEM-system collect events from various network security tools, aggregate them, lead to a common format and correlate (connect with each other in accordance with significant parameters) [2].

However, application of existing SIEM-systems methodology for security providing in IoT is not possible, due to specifics of IoT subject area. Existing SIEM systems are mostly focused on incidents detection in information systems. They are not designed for processing of large amounts of heterogeneous unstructured data; do not take into account fact that devices are controlled by each otherand logical connection between devices, which arises because devices perform a single technological-process.

Thus, there is need to develop new methods and approaches for processing large amounts of heterogeneous data and for detection of security incidents related to violations of the correctness of the technological process.

Ontological model of Internet of Things subject area for SIEM system development

Subject area model, which is based on ontologies, provides the following benefits, in accordance with [3, 4]:

- model could be easily adapted and supplemented, it is possible to define new terms without the need to revise existing definitions;
- it is possible to consider interconnected domain relations (internal and inter-level);
- it is possible to consider the same domain objects from different points of view at the expense of their affiliation to different conceptual constructions;
- it is possible to connect another models to ontological model, that are intended to describe individual subsystems domain using the concepts, that are introduced in ontological model;
- machine-readability and translatability of ontological model to other universal languages;
- it is possible to design a prototype of security system based on an ontological model.

Construction of ontological model for the Internet of Things allows to considerinteractions between devices, that implement physical processes through messaging, at different levels of abstraction. The result of ontological models creation are recommendations for functional characteristics of SIEM-system for the Internet of Things.

The overriding objective is a description of main (central) ontology concepts and relationships between them. Fig. 1 illus-

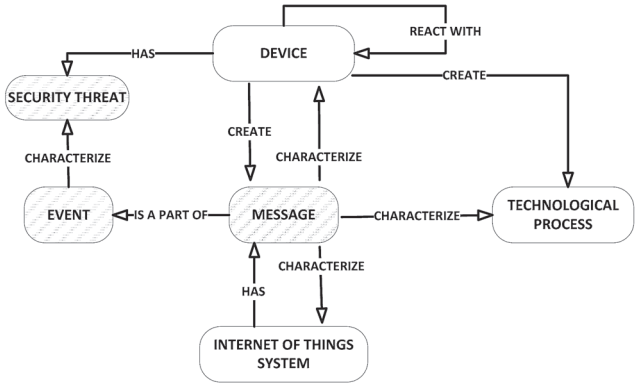


Fig. 1. Central ontology concepts

При финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП. «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014–2020 годы» (соглашение о предоставлении субсидии № 14.575.21.0100 от 14.11.2014 г., уникальный идентификатор RFMEFI57514X0100).

trates relationships between central ontology concepts, arrows symbolize dependence between concepts.

To reduce the dimension of messages space and their transformation to events space, it is advisable to consider in detail the concepts of "message" and "event" [5]. Level of messages and events is created, it is shown at Fig. 2.

Therefore, the dimension of messages space could be reduced by combining the values of messages into a single with an aggregation by time and by object type.

For development methods for detection of security incidents, which SIEM system should implement, concepts of "event" and "security threat" are considered, they are shown at Fig. 3.

This level reflects key characteristics of the anomalies in the IoT system. At the same time, it is reflected an important feature of IoT systems: there are two types of connections – communication and logical connections. Therefore, methods for detection of security incidents must take into account this feature.

Thus, developed ontological model has allowed to formulate recommendations to functional characteristics of SIEM-system for IoT, taking into account the specificity of the subject area.

Reduction of data dimension

The primary objective of SIEM system is problem of messages dimension reduction and of bringing them to a common format. To solve this problem, the technique of aggregation and normalization is proposed [6]. Techniqueinvolvesfollowing-steps:

• messages formats parsing and extraction of their parameters;

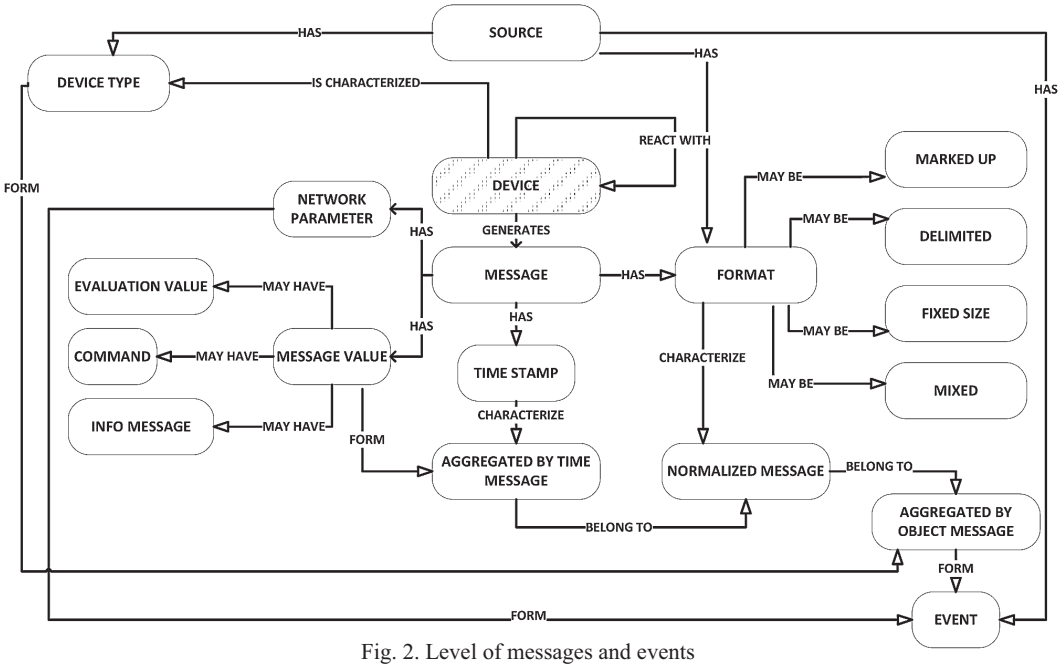


Fig. 2. Level of messages and events

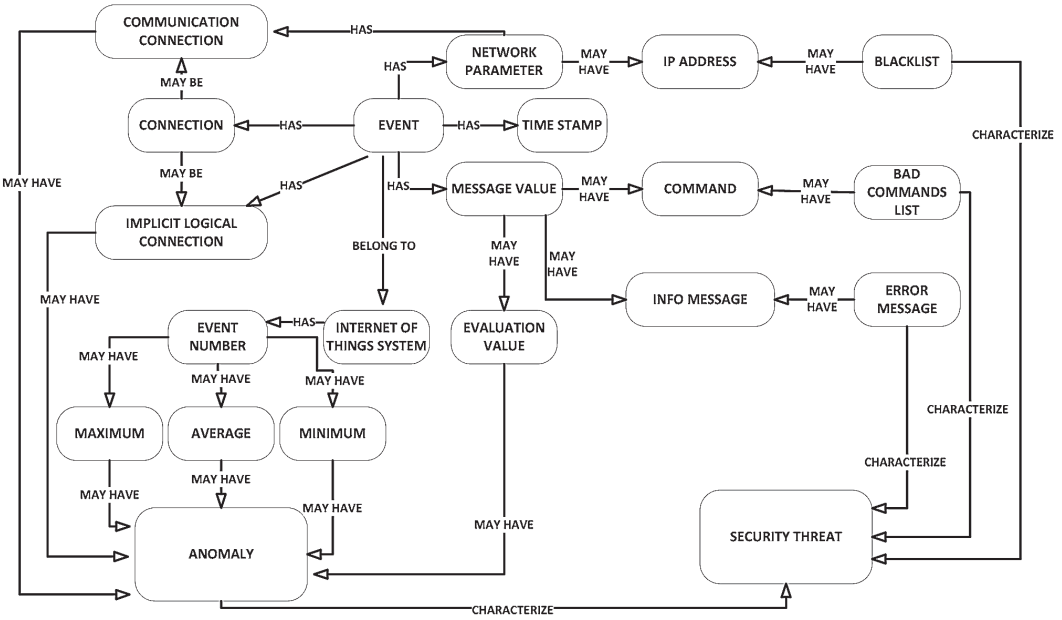


Fig. 3. Security threats level

• messages aggregation by time;
• messages parameters normalization and meta data assigning;
• messages aggregation in accordance with device type;
• events formation.

To parse messages formats and definitions of messages types metadata directories are used. These directories are used for messages parameters normalization, to determine to what format should be aligned parameters.

When messages areaggregated by time, parameters values, that are obtained from device for a certain period, are combined into one by using a statistical evaluation.

For more reduction of data dimension, aggregation by type of device is implemented. During such aggregation, the indicators of multiple devices of the same type are combined into one if their values are the same or different from each other less than the value of the error. However, such aggregation requires identical formats indicators, which is performed at data normalization stage. After messages aggregation by device type, messages are transformed to events. Event structure is described by a tuple of four elements (parameters that identify device-sender, device-receiver, type of event, time of event generation) [7].

Detection of security incidents in the Internet of Things

For detection of security incidents it is necessary to define the term "security event" for IoT. For security providing, effects of both information and processes in IoT system should be considered. To solve this problem, a set of interacting IoT devices is represented as a graph G, where devices are characterized by a set of vertices V, a set of edges E characterizes set of connections between devices [2]. Edges could be of two types:

• edges, that characterize communication links between devices during messaging;
• edges, that characterize logical connections between devices without exchanging messages.

Security event in IoT is a change in graph structure, which manifests itself in the change of the number of vertices, edges, and their parameters.

In accordance with graph model for IoT devices, for detection of security incidents is necessary to control the number of vertices and edges, and their parameters. Some parameters could be easily controlled using signature and statistical approaches [8].

However, control of connections and their parameters require being adapted to specific of IoT subject area. Therefore, it is proposed two methods for detection of security incidents:

• method based on self-similarity evaluation, for control of communication links;
• method based on dynamic similarity in data from pair of devices, for logical connections detecting and monitoring.

Idea of methodbased on self-similarity evaluation is that IoT system implements set of technological processes, each process is implemented with a certain periodicity. This periodicity is reflected in data of each device, which implements technological process. On this basis it is assumed a presence of self-similarity properties for time-series data from devices [9–14]. Security incident is considered to be a violation of self-similarity for time series generated by IoTdevice. Security criterion is value of the Hurst exponent, which takes the value between 0,5 and 1 for self-similar process [15]. Calculating the Hurst exponentis produced by dispersion method [16]:

1. For selected device is allocated a set of events for a certain period of time Δt;

2. Of events set are generated time series $x(t_1), x(t_2), ..., x(t_l)$, where x – values of events parameters at appropriate time;

3. Selected an aggregation period m and moved to aggregated time series $x^{(m)} : x_k^{(m)} = \frac{1}{m} \sum_{i=km-m+1}^{km} x_i$;

4. Plotted $\log D(x^{(m)})$ by $\log(m)$;

5. From ratio $\log D(x^{(m)})$ equivalent $\log D(x) - \beta \cdot \log(m)$ obtained value β;

6. Hurst exponentvalue calculated $H = 1 - \frac{\beta}{2}$.

The idea of method based on dynamic similarity in data is that during concerted work of devices data sets are changed rather similar [2, 17]. Security criterion for this method is deviation values from normal value of linear correlation coefficient and coefficient of agreement in dynamics [18]. Permissible deviation is determined in accordance with Chaddock scale: changing type of communication characterizes security incident [19].

Calculation of the linear correlation coefficient r occurs by formula

$$r = \frac{\sum_i (x_i - \overline{X})(y_i - \overline{Y})}{\sqrt{\sum_i (x_i - \overline{X})^2 (y_i - \overline{Y})^2}},$$

wherexandy – event parameters values from a pair of selected IoTdevices.

Coefficient of agreement in dynamics, in accordance with [20], occurs by formula

$$k_s = \frac{\sum_i \overline{\Delta}^i y \overline{\Delta}^i x}{\sqrt{\sum_i (\overline{\Delta}^i y)^2 \sum_i (\overline{\Delta}^i x)^2}},$$

where $\overline{\Delta}^i x$ and $\overline{\Delta}^i y$ – finite differences i-order [20].

Calculation of values for both coefficients allows to determine form of functional relationship between IoT devices. The dependence is linear if both coefficient values are near to 1, and if only the coefficient of agreement in dynamics value is near to 1, dependence is non-linear.

Experiments

To evaluate the effectiveness of developed methods was implemented experimental model of SIEM system. Research was performed on data obtained from self-regulating watering greenhouse system, they are shown at Fig. 4. System consisted of:

• soilmoisturesensors (400 pieces);
• temperatureSensors (400 pieces);
• lightsensors (270 pieces);
• „smart" cranes (20 pieces);
• leakagesensors (100 pieces).

Studies in reducing dimension of the data confirmed effectiveness of developed method of aggregation and normalization (Table).

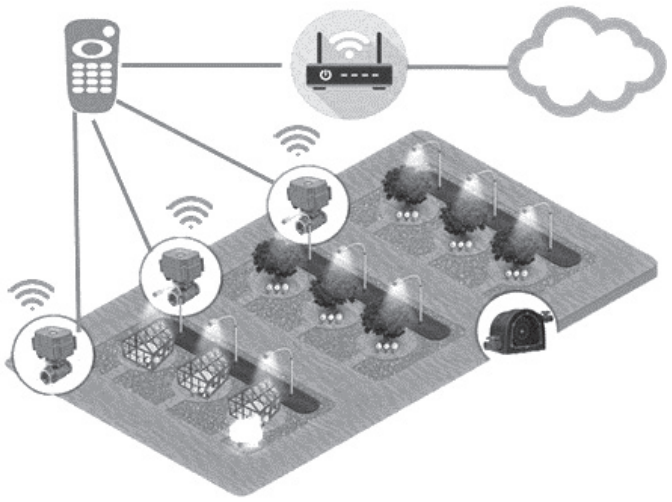


Fig. 4. Self-regulating watering greenhouse system

Table

The largest and smallest data reduction per day

Parameters	Light sensor	Soil moisture sensor
Frequency of messages generation	30 seconds	10 seconds
Aggregation period	2 minutes	30 seconds
Number of sensors	270 pieces	400 pieces
Amount of data per day	777 600 messages	3 456 000 messages
Amount of data after aggregation by time	194 400 messages	1 152 000 messages
% of aggregation by device type	68 %	43 %
Amount of data after aggregation by device type	59 320 messages	861 200 messages
Reduction of data amount	In 13,3 times	In 5 times

The best performance of data reduction per day were achieved for the light sensor because in most cases, both types of aggregation were performed. The worst results were obtained for the data of soil moisture sensors: as values did not coincide more than in 50 % of the cases, data volume declined by only in 5 times.

Evaluating the effectiveness of methods for detection ofsecurity incidents was carried out by implementing 60 attacks form the following classes:

- Denial of Service (DoS) – 9 attacks;
- Man-in-the-Middle (data interception, modification, deletion) – 34 attacks;
- system settings changing – 12 attacks;
- adding non-existent devices and data – 5 attacks.

Experiments have shown that developed methods could detect 95 % of attacks on IoT system, and the methods complement each other, detecting different types of attacks. In particular, data duplication attack to temperature sensor has been identified only by the method based on detection of implicit connections, as it was recorded violation of the implicit connection between a pair of temperature sensors. It should be noted that the attack of humidity sensor data modification, which was consisted in a smooth change of the observed values, was detected only by the method based on the self-similarity evaluation.

50 attacks were detected by method based on self-similarity evaluation, 39 attacks were detcted by method based on detecting implicit relations. Thus, 18 attacks were detected only by first method, and 7 attacks – by only second method. A total of 60 attacks were detected 57, for the entire SIEM system were detected errors: 9 % of first order, 5 % of second order.

2 of 3 missing attacks belonged to “Man-in-the-Middle” class. They have not been detected due to the fact that in database was not implemented records of minimum and maximum values of parameters for each aggregation period. Last one attack belonged to “system settings changing”class, it has not been detected due to a short training period for system, so not all implicit connections were found.

The results indicate that developed methods allow full use for detection of security incidents in IoT.

Conclusion

Thus, has been developed an approach for detection of security incidents in IoT based on SIEM technology. The approach takes into account the specifics of IoT subject area, which is in the large amounts of heterogeneous data from devices and in need to control not only communication, but also the logical connections between devices. Experimental results showed that developed detection methods are able to detect security incidents that are not detectable by standard methods used in SIEM-systems.

Future work will be related to the study of the safety of cyberphysical systems and the development of a dynamic approach to assessing the safety of complex systems.

References

1. Vermesan O., Friess P. Internet of Things Applications – From Research and Innovation to Market Deployment, Bringing IP to Low-power Smart Objects: The Smart Parking Case in the CALIPSO Project, *The River Publishers, Series in Communications*, 2014, pp. 287-313.

2. Lavrova D. S. Podhod k razrabotke SIEM-sistemy dlya InternetaVeshchej [Approach to development a SIEM-system for the Internet of Things], *Problemy informacionnoj bezopasnosti. Komp'yuternye sistemy*, 2016, no. 2, pp. 50-60.

3. Poletaeva E. V. Principy postroeniya ontologii predmetnoj oblasti mashinostroeniya [Principles for construction of ontologies for engineering subject domain]. *Programmnye produkty, sistemy i algoritmy* [Software Products, Systems and Algorithms], 2015, no. 1.

4. Lychkina N. N., Idiatullin A. R. Razrabotka kompleksa ontologicheskih modelej arhitektury predpriyatiya [Development of a complex of ontological models of enterprise architecture], *V Int. Conf. Parallel'nye vychisleniya i zadachi upravleniya* [Parallel Comput. Control Tasks], Moscow, 2010.

5. Lavrova D. S. Ontologicheskaya model' predmetnoj oblasti Interneta veshchej dlya analiza bezopasnosti [Ontological Internet of Things domain model for security analysis], *Problemy informacionnoj bezopasnosti. Komp'yuternye sistemy* [Inf. Security Prob. Comput. System], 2016, no. 2, pp. 68-75.

6. Poltavceva M. A. Normalizaciya dannyh Interneta veshchej v sisteme obnaruzheniya incidentov bezopasnosti. Internet of Tnings date normalization for detection of security incidents], *24 Sci. Tech. Conf. "Metody i tekhnicheskie sredstva*

obespecheniya bezopasnosti informacii" [Methods and Tech. Means of Inf. Secur.] 29 June – 02 July 2015, St. Petersburg, Izdatel'stvo Politekhnicheskogo universiteta, 2015, pp. 29-31.

7. Lavrova D., Pechenkin A. Applying Correlation and Regression Analysis Methods for Security Incidents Detection in the Internet of Things, *Int. J. Commun. Netw. Inf. Secur*, 2015, Vol. 7, no. 3, pp. 131-137.

8. Nadezhdin E. N., Cvetkov A. A. Sintez programmy monitoringa resursov vychislitel'noj seti obrazovatel'noj organizacii [Synthesis of program for monitoring resources of computer network of educational organization], *Naukovedenie* [Naukovedenie], 2014, no. 5 (24). Available at: http://go-url.ru/sintez (accessed 04.09.2016).

9. Fedorova M. L., Ledeneva T. M. Ob issledovanii svojstva samopodobiya trafika mul'tiservisnoj seti [About the investigation of the self-similarity property of traffic of a multiservice network]. Available at: http://www.vestnik.vsu.ru/pdf/analiz/2010/01/2010-01-09.pdf (accessed 28.04.2015).

10. Trenogin N. G., Sokolov D. E. Fraktal'nye svojstva setevogo trafika v klient-servernoj informacionnoj sisteme [Fractal properties of network traffic in the client-server information system], *Vestnik SibGUTI [The Herald og SibSUTIS]*, 2003, pp. 163-172.

11. Girik A. V. Obnaruzhenie informacionnyh ugroz bezopasnosti peredachi dannyh v telekommunikacionnyh setyah [Detection of information threats to the security of data transmission in telecommunication networks], *XV All-Russian Sci. Metod. Conf. „Telematika-2008",* St. Petersburg, 23–26 Juni 2008, St. Petersburg, 2008, p. 178.

12. Loktev A. A., Zaletdinov A. V. Ispol'zovanie fraktalov v zadachah obespecheniya informacionnoj bezopasnosti [The use of fractals in the tasks of ensuring information security], *Vestnik Tambovskogo universiteta. Estestvennye i tekhnicheskie nauki* [Tambov Univ. Rep. Series Sci. Natur. Sci.], 2010, Vol. 2, is. 2, pp. 442-447.

13. Lavrova D. S., Zegzhda D. P., Zegzhda P. D., Shtyrkina A. A. Ocenka kiberustojchivosti informacionno-tekhnologicheskih sistem na osnove samopodobiya [Cyber-resistance assessment of information technology systems on the basis of self-similarity], *25 Sci. Tech. Conf. „Metody i tekhnicheskie sredstva obespecheniya bezopasnosti informacii"* [Methods and Tech. Means of Inf. Secur.], St. Petersburg, Izdatel'stvo Politekhnicheskogo universiteta, 2016, pp. 101-104.

14. Dejneko Zh. V., Zamula A. A., Kirichenko L. O., Radivilova T. A. Ob odnom metode modelirovaniya samopodobnogo stohasticheskogo processa [About one method of modeling a self-similar stochastic process], *Visnik Harkovskogo nacionalnogo universitetu imeny V. N. Karazina. Matematichne modelyuvannya. Informacijni tekhnologiï. Avtomatizovani sistemi upravlinnya* [Bul. V. N. Karazin Kharkiv Nat. Univ. Sci. Periodicals, series "Math. Modeling. Inf. Technol. Automated Control Systems"], 2010, Vol. 13, no. 890, pp. 53-63.

15. Shibaeva E. S. Sravnenie metodov analiza pokazatelya Hersta dlya fraktal'nogo setevogo trafika [Comparison of methods of analysis of the Hurst exponent for fractal network traffic]. Available at: http://www.mce.su/archive/doc97687/doc.pdf (accessed 28.06.2016).

16. Pechenkin A. I., Gluhov V. V., Lavrova D. S. Applying Correlation Analysis Methods to Control flow Violation Detection in the Internet of Things, *Autom. Control Comput. Sci*, 2015, no. 8, pp. 735-740.

17. Pechenkin A. I., Lavrova D. S. Rassledovanie incidentov bezopasnosti v InterneteVeshchej s ispol'zovaniem korrelyacionno-regressionnogo analiza [Investigation of security incidents on the Internet of things using correlation-regression analysis], *IX St. Peterburg. Int. Conf. „Informacionnaya bezopasnost' regionov Rossii (IBRR-2015)"* [Inform. Security of the Regions of Russia], St. Petersburg, 28–30 Okt. 2015, St. Petersburg, SPOISU, 2015, p. 110.

18. Svetun'kov S. G., Svetun'kov I. S. Metody social'no-ehkonomicheskogo prognozirovaniya [Methods of socio-economic forecasting], t. 1, St. Petersburg, Izdatel'stvo SPbGUEHF, 2009, pp. 254-268.

19. Chaddock R. E. Principles and Methods of Statistics, 1st ed., Cambridge, Houghton Miffin Comp., The Riverside Press, 1925.

20. Gel'fond A. O. Ischislenie konechnyh raznostej [Finite difference calculus], Moscow, Librokom, 2012.

Подход к обнаружению инцидентов безопасности в Интернете вещей с использованием технологии SIEM

Зегжда Д. П., Лаврова Д. С.
Санкт-Петербургский политехнический университет Петра Великого
Санкт-Петербург, Россия
dmitry.zegzhda@ibks.ftk.spbstu.ru, lavrova@ibks.spbstu.ru

Аннотация. **В данной статье предлагается подход к обнаружению инцидентов безопасности в Интернете вещей с использованием технологии SIEM. Предлагаемый подход учитывает такие особенности предметной области Интернета вещей, как высокая разнородность устройств и большое количество неявных логических связей, возникающих между устройствами при реализации ими технологических процессов. Также формализовано понятие события безопасности для Интернета вещей на основе графовой модели взаимодействия устройств.**

Ключевые слова: **Интернет вещей, инцидент безопасности, SIEM, анализ безопасности, агрегация данных.**

References

1. Vermesan O. Internet of Things Applications – From Research and Innovation to Market Deployment, Bringing IP to Low-power Smart Objects: The Smart Parking Case in the CALIPSO Project / O. Vermesan, P. Friess // The River Publishers, Series in Communications. – 2014. – P. 287–313.

2. Лаврова Д. С. Подход к разработке SIEM-системы для Интернета вещей / Д. С. Лаврова // Проблемы информационной безопасности. Компьютерные системы. – 2016. – № 2. – С. 50–60.

3. Полетаева Е. В. Принципы построения онтологии предметной области машиностроения / Е. В. Полетаева // Программные продукты, системы и алгоритмы. – 2015. – № 1.

4. Лычкина Н. Н. Разработка комплекса онтологических моделей архитектуры предприятия / Н. Н. Лычкина, А. Р. Идиатуллин // V междунар. конф. «Параллельные вычисления и задачи управления». – М., 2010.

5. Лаврова Д. С. Онтологическая модель предметной области Интернета вещей для анализа безопасности / Д. С. Лаврова // Проблемы информационной безопасности. Компьютерные системы. – 2016. – № 2. – С. 68–75.

6. Полтавцева М. А. Нормализация данных Интернета вещей в системе обнаружения инцидентов безопасности / М. А. Полтавцева // Сб. материалов 24-й науч.-технич. конф. «Методы и технические средства обеспечения безопасности информации» 29 июня – 02 июля 2015 г. – СПб.: Изд-во Политех. ун-та, 2015. – С. 29–31.

7. Lavrova D. Applying Correlation and Regression Analysis Methods for Security Incidents Detection in the Internet of Things / D. Lavrova, A. Pechenkin // Int. J. Commun. Netw. Inf. Secur. – 2015. – Vol. 7, no. 3. – P. 131–137.

8. Надеждин Е. Н. Синтез программы мониторинга ресурсов вычислительной сети образовательной организации / Е. Н. Надеждин, А. А. Цветков // Науковедение. – 2014. – № 5 (24). – URL: http://go-url.ru/sintez (дата обращения 04.09.2016).

9. Федорова М. Л. Об исследовании свойства самоподобия трафика мультисервисной сети / М. Л. Федорова, Т. М. Леденева. – URL: http://www.vestnik.vsu.ru/pdf/analiz/2010/01/2010-01-09.pdf (дата обращения 28.04.2015).

10. Треногин Н. Г. Фрактальные свойства сетевого трафика в клиент-серверной информационной системе / Н. Г. Треногин, Д. Е. Соколов // Вестн. СибГУТИ. – 2003. – С. 163–172.

11. Гирик А. В. Обнаружение информационных угроз безопасности передачи данных в телекоммуникационных сетях / А. В. Гирик // Тез. докл. XV всерос. науч.-метод. конф. «Телематика-2008», СПб., 23–26 июня 2008 г. – СПб., 2008. – С. 178.

12. Локтев А. А. Использование фракталов в задачах обеспечения информационной безопасности / А. А. Локтев, А. В. Залетдинов // Вестн. Тамбов. ун-та. Естественные и технические науки. – 2010. – Т. 2, вып. 2. – С. 442–447.

13. Зегжда Д. П. Оценка киберустойчивости информационно-технологических систем на основе самоподобия / Д. П. Зегжда, П. Д. Зегжда, А. А. Штыркина, Д. С. Лаврова // Материалы 25-й науч.-технич. конф. «Методы и технические средства обеспечения безопасности информации». – СПб.: Изд-во Политех. ун-та, 2016. – С. 101–104.

14. Дейнеко Ж. В. Об одном методе моделирования самоподобного стохастического процесса / Ж. В. Дейнеко, А. А. Замула, Л. О. Кириченко, Т. А. Радивилова // Вісн. ХНУ ім. В. Н. Каразіна. Математичне моделювання. Інформаційні технології. Автоматизовані системи управління. – 2010. – № 890, вип. 13. – С. 53–63.

15. Шибаева Е. С. Сравнение методов анализа показателя Херста для фрактального сетевого трафика [Элек-

тронный ресурс] / Е. С. Шибаева. – URL: http://www.mce.su/archive/doc97687/doc.pdf (дата обращения 28.06.2016).

16. Pechenkin A. I. Applying Correlation Analysis Methods to Control flow Violation Detection in the Internet of Things / A. I. Pechenkin, V. V. Gluhov, D. S. Lavrova // Autom. Control Comput. Sci. – 2015. – № 8. – P. 735–740.

17. Лаврова Д. С. Расследование инцидентов безопасности в Интернете Вещей с использованием корреляционно-регрессионного анализа / А. И. Печенкин, Д. С. Лаврова // IX Санкт-Петербург. межрегион. конф. «Информационная безопасность регионов России (ИБРР-2015)», СПб., 28–30 окт. 2015 г.: материалы конф. – СПб.: СПОИСУ, 2015. – С. 110.

18. Светуньков С. Г. Методы социально-экономического прогнозирования: учеб. для вузов. Т. 1 / С. Г. Светуньков, И. С. Светуньков. – СПб.: Изд-во СПбГУЭФ, 2009. – С. 254–268.

19. Chaddock R. E. Principles and Methods of Statistics / R. E. Chaddock. – 1st ed. – Cambridge: Houghton Miffin Company, The Riverside Press, 1925.

20. Гельфонд А. О. Исчисление конечных разностей / А. О. Гельфонд. – М.: Либроком, 2012.

Обзор автоматизированных систем мониторинга

Носкова А. И., Токранова М. В.
Петербургский государственный университет путей сообщения Императора Александра I
Санкт-Петербург, Россия
magistrpgups@rambler.ru

Аннотация. **Дана общая классификация автоматизированных систем мониторинга (АСМ), рассмотрены основные аспекты их применения. В связи с непрерывным масштабным построением крупных стратегически важных объектов и развитием современных технологий АСМ автоматизируют и значительно упрощают этот процесс, улучшая качество наблюдения и точность собранных данных мониторинг является важным процессом современного промышленного производства. В статье рассмотрены основные сферы применения АСМ, а также примеры популярных систем на рынке: деформационного мониторинга, мониторинга окружающей среды, транспорта, ИТ-систем.**

Ключевые слова: **автоматизированные системы мониторинга, деформационный мониторинг, мониторинг окружающей среды, мониторинг транспорта, мониторинг ИТ-систем.**

Введение

Окружающий мир находится в непрерывном изменении, меняется среда обитания людей, стиль и качество их жизни. Возникает множество небоскребов, тоннелей длиной в несколько километров, мостов, соединяющих острова, обостряется проблема безопасности жизни и деятельности человека. Появляются новые технологии и установки, которые не всегда полезны для экологии; происходят вредные выбросы в окружающую среду, загрязняются водоёмы; вымирают редкие виды животных. Из-за бурного развития промышленности используется много горючих материалов, электроэнергии. Часто возникают пожары. Контроль и прогнозирование этих процессов – сложный процесс. Специалисты по всему миру ведут постоянные наблюдения. Их интересуют как количественные, так и качественные показатели. Для обозначения этого процесса используют термин «мониторинг» (от лат. *monitor* – наблюдение, контроль, предостережение).

Мониторинг – это непрерывный процесс наблюдения и регистрации параметров объекта в сравнении с заданными критериями [1]. Сегодня этот термин используется в медицине, в метеорологии, в строительстве и т. д. В некоторых отраслях данные собираются и накапливаются очень интенсивно.

Сегодня создано множество технологий на базе геодезических приборов, позволяющих проводить мониторинг важных объектов с высокой точностью в реальном времени для предупреждения катастроф и аварий. Эти технологии основаны на сборе данных от измерительных приборов (сенсоров), в числе которых имеются геодезические, в частности GPS-оборудование. Сведения от всех сенсоров передаются в единую базу данных и совместно обрабатываются [2].

Для управления датчиками на большом расстоянии от места сбора и обработки данных используются системы автоматизированного мониторинга. Работающая в автоматическом режиме система позволяет выполнять циклы измерений с высокой скоростью и исключать ошибки, связанные с человеческим фактором. Промежутки между циклами измерений могут составлять от нескольких минут или часов до месяцев и лет. В списке задач, решаемых человеком, остаются качественный анализ собранных результатов, выбор необходимых средств наблюдений, их расположения и соединения в общую сеть. Имея постоянно обновляемые параметры наблюдаемого объекта, можно с высокой степенью достоверности прогнозировать состояние наблюдаемого объекта, предотвращать аварии или рассчитывать экономические показатели последствий происшествий [3, 4].

Основные преимущества использования систем автоматизированного мониторинга:

- контроль данных в реальном времени с удаленного места;
- непрерывный мониторинг объектов;
- доступное расположение сенсоров измерительной системы, не зависящее от ручного управления оператором;
- сбор данных, предварительный анализ информации и ее отправка в любое место через Интернет;
- автоматическое уведомление лиц о любом смещении за пределы установленного диапазона;
- экономия денежных средств, поскольку автоматические наблюдения позволяют отказаться от участия человека;
- исключение ошибок оператора, так как автоматические наблюдения более достоверны.

Автоматизированные системы деформационного мониторинга

Построено уже большое количество стратегически важных объектов, таких как плотины, дамбы, ГЭС, АЭС, телевизионные вышки, старение конструкций которых требует особого внимания. Разрушаются мосты и жилые здания, выходят из строя линии электропередачи, происходят обвалы в шахтах. Есть множество факторов, влияющих на решение данной задачи. К ним можно отнести природные катастрофы и катаклизмы, техногенные аварии, повышенные нагрузки, ошибки в проектировании и строительстве [5].

Вместе с тем, большого внимания требуют такие природные явления, как движения земной коры, оползни, вулканическая деятельность, землетрясения, которые нуждаются в изучении для прогнозирования и предупреждения чрезвычайных ситуаций. Контроль стабильности потенциально опасных объектов и прогнозирование их поведения – очень серьезные вопросы. Решением таких инженерных задач является определение процессов деформации, оседания, изменения структуры предметов. Мониторинг состояния природных объектов и ис-

кусственных сооружений в наши дни – необходимая и неотъемлемая часть системы обеспечения безопасности [6, 7].

Одна из лидирующих компаний в области деформационного мониторинга – LeicaGeoMoS (Швейцария). Ее современная программная система мониторинга, конфигурируемая под конкретное применение, используется на существующих и строящихся объектах любой величины, обеспечивает функционирование очень гибкой автоматической системы контроля деформаций, которая позволяет комбинировать сведения от различных датчиков (GNSS-приемников, тахеометров, геотехнических и метеорологических сенсоров) [8]. LeicaGeoMoS применяется для контроля за структурными деформациями (дамб, плотин, насыпей, тоннелей, мостов, высотных зданий), за оползнями и осадками (оседанием породы или просадкой грунта), автоматизированной съемки (например, непрерывных, автоматизированных измерений) [9].

Программное обеспечение LeicaGeoMoS состоит из нескольких приложений:

• GeoMoSMonitor работает в режиме реального времени, собирает, обрабатывает и накапливает данные, отображает их на экране, проверяет данные на вхождение в установленные допуски и оповещает определенных лиц;

• GeoMoSAnalyzer работает в автономном режиме, предназначено для просмотра и анализа накопленных данных;

• GeoMoSHiSpeed собирает и обрабатывает данные от GNSS-приёмников в высоком темпе (до 20 Гц), предназначено для профессионального принятия решения, основанного на анализе больших потоков данных;

• GeoMoSAdjustment отвечает за вычисление сетевых поправок (уравнивание), анализ деформаций и сетевое моделирование.

LeicaGeoMoS хранит все измерения и результаты обработки в открытой базе данных MySQL, к которым можно обратиться локально или удаленно, используя приложения LeicaGeoMoSAnalyzer, LeicaGeoMoSAdjustment или иное программное обеспечение [9].

Для точного установления причин обнаруженного движения и прогнозирования развития событий LeicaGeoMoS соединяет в систему геодезические (электронные тахеометры и датчики GNSS) и геотехнические датчики:

• тахеометры серий Leica TM50, TS50, TS15, TM30, TS30, TPS1100, TPS1200, TPS1200+, TCA1201M, TPS1800 и TCA2003, TPS LeicaViVa;

• мультистанцию Leica MS50;

• спутниковые GNSS-датчики GPS SystemLeicaViVa, серию GMX900;

• Leica GNSS Spider для расширенного GNSS-мониторинга;

• нивелиры Leica DNA и Leica Sprinter;

• датчики наклона Leica Nivel210/220;

• метеорологические датчики (температура, давление и т. п.);

• интерфейс для подключения регистраторов данных CampbellScientific: геотехнические датчики для измерения влияния внешних условий, например, экстензометры (для измерения линейных деформаций), пьезометры (для измерения сжимаемости газов), датчики напряжения, инклинометры, термометры, барометры, датчики дождя и другие [8].

В дополнение к стандартным средствам связи LeicaGeoMoS также поддерживает сетевой протокол связи TCP/IP, который позволяет использовать технологию Ethernet и мобильные сети.

Автоматизированные системы мониторинга окружающей среды

Ухудшение состояния природной среды, как правило, связано с нерациональным и варварским использованием ресурсов, с ошибками в технической и экологической политике, с низким уровнем разработки и внедрения безотходных технологий, с малой изученностью всех последствий антропогенного воздействия. В сложившейся ситуации чрезвычайно важны для практических действий и долгосрочного прогнозирования качества окружающей среды контроль состояния и определение тенденций ее изменения [10].

Наблюдение за состоянием окружающей среды представляет собой сбор информации о фактическом состоянии объектов окружающей среды, об источниках загрязнения, об основных изменениях под воздействием загрязнителей. На основе этой информации анализируются процессы, составляются прогнозы изменения среды и планы предотвращения отрицательных последствий, разрабатываются стратегии оптимальных взаимоотношений общества и окружающей среды [11].

Рассмотрим одну из систем экологического мониторинга – Emercit (ИАС ЭМЕРСИТ). Эта информационно-аналитическая система предназначена для организации территориально распределенного оперативного контроля состояния окружающей среды с целью обнаружения и прогнозирования опасных явлений и процессов [12]. Система позволяет в реальном времени производить измерения и передавать их результаты в центр мониторинга (ситуационный центр) или в дежурно-диспетчерскую службу (ЕДДС). Фиксируются следующие основные параметры:

• уровень зеркала воды рек и открытых водоемов;

• количество и интенсивность жидких осадков;

• мощность фонового эквивалента дозы гамма-излучения;

• содержание аварийно-химических опасных и токсичных веществ в атмосферном воздухе;

• наличие и концентрация газов углеводородной группы в атмосфере;

• наличие в атмосфере боевых отравляющих веществ;

• скорость и направление ветра, температура и относительная влажность атмосферного воздуха, атмосферное давление;

• высота снежного покрова;

• температура на поверхности почвы и на заданной глубине;

• суммарная солнечная радиация.

Если один из наблюдаемых параметров выходит за пределы нормы, то система генерирует тревожное сообщение, соответствующее наступлению неблагоприятного или опасного явления. При фиксации опасного уровня показателей состояния окружающей среды измерительные комплексы автоматически переходят в учащенный режим измерения.

В зависимости от задач посты наблюдения Emercit могут быть укомплектованы различными метеорологическими датчиками [12]. В стандартную поставку постов наблюдения Emercit входят следующие датчики:

• количества (интенсивности) и вида осадков. Способен различать пять видов осадков: дождь, снег, град, снег с дождем, морось (радиолокационным методом измерения);

• скорости и направления ветра (ультразвуковым методом измерения);

• атмосферного давления, температуры и влажности воздуха.

Автоматизированные системы мониторинга транспорта

Определение местоположения подвижного объекта, скорости его перемещения и точного времени с использованием технологий спутниковой навигации широко применяется в системах мониторинга транспорта. Сейчас применение технологий автоматизированного спутникового слежения и контроля – незаменимая составляющая бизнес-процесса на предприятии, цель которого – поднять управление автопарком на новый эффективный уровень.

Технологии спутникового мониторинга транспорта активно развиваются. Первоначально системы мониторинга применялись исключительно для контроля или мониторинга перемещения транспортных средств и работали только в офлайн-режиме, не позволяя в реальном времени следить за объектом. С развитием технологий передачи данных GSM/GPRS, а также web-технологий системы мониторинга автотранспорта позволили дистанционно наблюдать за транспортом круглосуточно, практически в реальном времени.

В системах мониторинга и контроля транспорта используется сочетание навигационных и телекоммуникационных технологий. К примеру, в качестве каналов передачи данных в основном используется GSM/GPRS, а в отдаленных районах, где отсутствует покрытие сотовой связи – системы спутниковой связи [13].

Развитие технологий также позволило использовать в системе мониторинга телеметрию объектов. Стало возможным подключение различных датчиков и исполнительных устройств, которые позволяют или подавать водителю сигналы тревоги в режиме реального времени, или отслеживать заправку и слив топлива (датчик уровня топлива), либо датчиков состояния механизмов, к примеру, измерители температуры, концевые выключатели и т. д. В последнее время стали популярны средства фото- и видеофиксации [14].

Концепция «Интернет вещей»

Концепция Интернета вещей (Internet of Things – IoT) представляет собой систему, которая имеет собственную среду и протокол. Внешний слой этой среды – комплексные системы управления – механические, тепловые, оптические и другие датчики, которые измеряют физическое состояние зданий, оборудования или даже людей. Благодаря встроенным датчикам и микропроцессам IoT устройства приобретают способность ощущать окружающую среду и обмениваться данными с компьютером или другим оборудованием. «Умные вещи» получают сигналы и выполняют задачи, не требуя при этом ввода информации человеком. Идеология Интернета вещей направлена на повышение эффективности за счет автоматизации процессов в различных сферах деятельности, в том числе мониторинга, исключая человека [15].

Потенциальные возможности применения IoT многочисленны и разнообразны. Они проникают практически во все сферы повседневной жизни людей, предприятий и общества в целом:

• здравоохранение. IoT-платформы обеспечивают централизованный мониторинг и агрегацию данных медицинского оборудования и приложений;

• торговля. Интернет вещей позволяет внедрять высокие технологии на предприятиях розничной и оптовой торговли, предлагая решения по автоматизации производства;

• сельское хозяйство. IoT-платформа позволяет автоматизировать множество аспектов деятельности сельхозпроизводства, повышая эффективность и финансовые показатели на производстве.

Сферы применения Интернета вещей не ограничиваются указанными, в каждой можно найти наиболее эффективный сценарий использования (рис. 1).

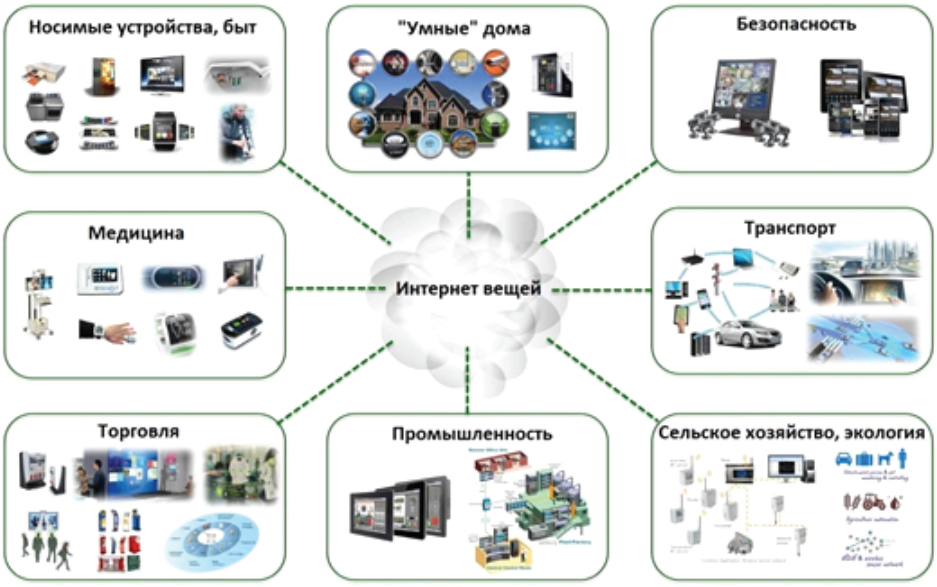


Рис. 1. Сферы применения Интернета вещей

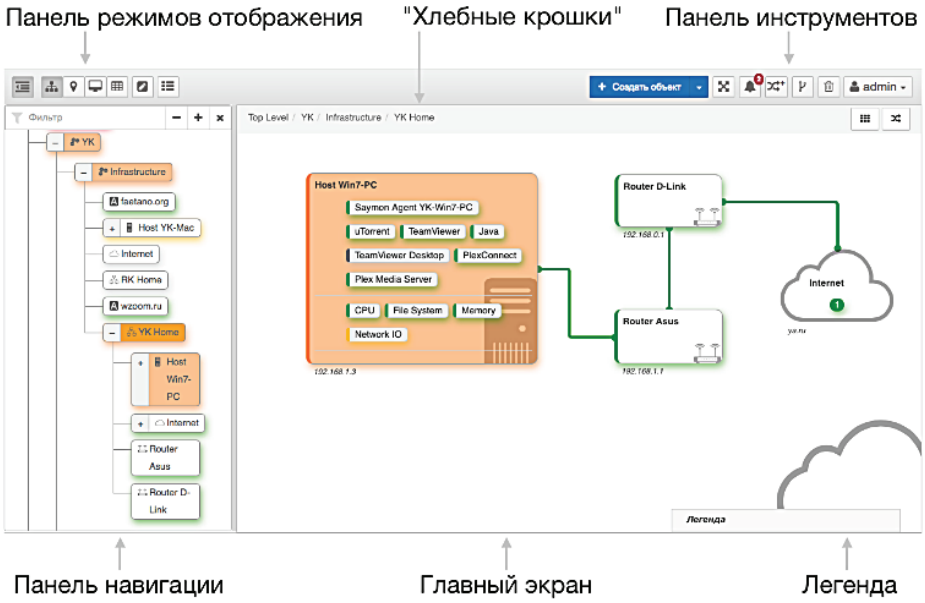


Рис. 2. Веб-интерфейс SAYMON

Понятие Интернета вещей можно условно разделить на две сферы применения: бытовые сети «умных» вещей (adhocIoT) и интеллектуальные решения в области межмашинных коммуникаций Machine-to-Machine (M2M).

AdhocIoT – концепция Интернета вещей интеллектуальной окружающей среды, основанной на ситуативных децентрализованных беспроводных сетях (adhoc). Эта среда состоит из привычных, но «улучшенных» бытовых вещей.

Но особую роль в развитии IoT играет интеллектуальное решение в области M2M. M2M – общее название технологий, которые позволяют приборам обмениваться информацией друг с другом. Это проводные и беспроводные системы датчиков, которые передают информацию от одного устройства другому. С помощью решений IoT/M2M компании смогут удаленно проверять состояние своего оборудования, степень износа, вероятность сбоев, контролировать многие другие показатели.

Залогом успешного функционирования IoT является качественное и надежное взаимодействие как отдельных приборов, так и объединенных групп устройств, находящихся под постоянным контролем, поэтому платформа мониторинга и управления становится еще одним сегментом концепции Интернета вещей, без которой успешная работа системы невозможна.

Примером такой платформы мониторинга является SAYMON, предназначенная для постоянного и статистического наблюдения и контроля состояния показателей работы сети, оборудования, приложений и сервисов. SAYMON предоставляет богатый инструментарий для управления и мониторинга сетями устройств, обработки и анализа данных, интеграции с другими системами предприятия [16] (рис. 2).

Объектом мониторинга может быть любой объект физического или логического мира, например, память, процессор, файловая система, процесс или программа, количество пользователей, очередь файлов на обработку, объем обработанного трафика, выручка и иные финансовые показатели, значение температуры или химического состава газа или жидкости [17].

Отличительной особенностью платформы является возможность хранения оригинальных немодифицированных значений показателей за значительные промежутки времени с обеспечением высокой скорости записи и доступа к данным, что позволяет быстро и качественно анализировать ситуации в настоящем и прошлом, строить математически обоснованные прогнозы развития ситуации в будущем [16].

Заключение

Подводя итоги, можно сказать, что по мере модернизации производства, масштабного строения крупных стратегически важных объектов и развития современных технологий автоматизированные системы мониторинга применяются все шире. АСМ позволяют постоянно удаленно контролировать объекты, упрощая этот процесс для человека, способствуют уменьшению количества ошибок, связанных с человеческим фактором. Но с ростом роли АСМ необходимо уделять больше внимания вопросам правильной работы систем и защиты получаемых данных.

Литература

1. https://en.wikipedia.org/wiki/System_monitoring (дата обращения 10.09.2016).

2. Dunnicliff J. Geotechnical Instrumentation For Monitoring Field Performance / J. Dunnicliff. – 2010. – P. 113–185.

3. Funk P., Xiong N. Why we need to move to intelligent and experience based monitoring and diagnostic systems / P. Funk, N. Xiong // Proc. 23th Int. Conf. Condition Monitoring and Diagnostic Eng. Management. – 2010. – P. 111–115.

4. Хорошилов В. С. О разработке информационной экспертной системы для оптимального геодезического обеспечения инженерных объектов / В. С. Хорошилов // Геодезия и картография. – 2008. – № 5. – С. 15–19.

5. http://www.icentre-gfk.ru (дата обращения 15.09.2016).

6. Moore J. F. A. Monitoring Building Structures / J. F. A. Moore. – Blackie and Son Ltd. – 2009. – P. 93–136.

7. Kopáčik A. New Trends of Automated Bridge Monitoring / A. Kopáčik, P. Kyrinovič, J. Erdélyi, I. Lipták // Reportson Geodesy. – 2011. – № 1 (90). – P. 173–181.

8. http://leica-geosystems.com (дата обращения 15.09.2016).

9. http://www.gfk-leica.ru (дата обращения 15.09.2016).

10. Ясовеев М. Г. Экологический мониторинг и экологическая экспертиза: учеб. пособие / М. Г. Ясовеев, Н. Л. Стреха, Э. В. Какарека, Н. С. Шевцова; под ред. проф. М. Г. Ясовеева. – М.: НИЦ ИНФРА-М, Новое знание, 2013. – 304 с.

11. Косинова И. И. Иерархическая структура эколого-геологического мониторинга / И. И. Косинова // Мониторинг геологических, литотехнических и эколого-геологических систем. – М.: МГУ, 2007. – С. 24–25.

12. http://www.emercit.ru (дата обращения 20.09.2016).

13. Харисова В. Н. Глобальная спутниковая радионавигационная система ГЛОНАСС / В. Н. Харисова. – М.: ИПРЖР, 2011.

14. http://mssglonass.ru (дата обращения 30.09.2016).

15. http://www.rfidjournal.com/articles/view?4986 (дата обращения 25.03.2017).

16. http://www.saymon.info (дата обращения 25.03.2017).

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

Overview of Automated Monitoring Systems

Noskova A. I., Tokranova M. V.
Emperor Alexander I St. Petersburg State Transport University
St. Petersburg, Russia
magistrpgups@rambler.ru

Abstract. **The general classification of automated monitoring systems (ACM), the main aspects of their application are considered. Monitoring is an important process for modern industrial production, due to the continuous large-scale construction of large strategically important facilities and the development of modern technologies. This led to the creation of systems that automate and greatly simplify this process, at the same time improving the quality of observations and the accuracy of the data collected. Thanks to ASM the person to carry out the analysis of the acquired information. The article tells about the main scope of the ASM and the examples of the most popular systems on the market.**

Keywords: **automated monitoring system, deformation monitoring, environmental monitoring, traffic monitoring, monitoring of IT systems.**

References

1. https://en.wikipedia.org/wiki/System_monitoring (accessed 14.09.2016).

2. Dunnicliff J. Geotechnical Instrumentation For Monitoring Field Performance, 2010, pp. 113-185.

3. Funk P., Xiong N. Why we need to move to intelligent and experience based monitoring and diagnostic systems, *Proc. 23th Int. Conf. Condition Monitoring and Diagnostic Eng. Management*, 2010, pp. 111-115.

4. Khoroshilov V. S. O razrabotke informacionnoj ehkspertnoj sistemy dlya optimal'nogo geodezicheskogo obespecheniya inzhenernyh ob"ektov [On the development of the information system of the expertnoy to ensure optimal geodetic engineering facilities], *Geodesy and Cartography [Geodeziya i kartografiya]*, 2008, no. 5, pp. 15-19.

5. http://www.icentre-gfk.ru (accessed 15.09.2016).

6. Moore J. F. A. Monitoring Building Structures. Blackie and Son Ltd., 2009, pp. 93-136.

7. Kopáčik A., Kyrinovič P., Erdélyi J., Lipták I. New Trends of Automated Bridge Monitoring, *Reportson Geodesy*, 2011, no. 1 (90), pp. 173-181.

8. http://leica-geosystems.com (accessed 15.09.2016).

9. http://www.gfk-leica.ru (accessed 15.09.2016).

10. Yasoveyev M. G., Strekha N. L., Kakareka E. V., Shevtsova N. S. Ekologicheskiy monitoring i ekologicheskaya ekspertiza [Environmental Monitoring and Environmental Impact Assessment]: ed. prof. M. G. Yasoveyev, Moscow, NITS INFRA-M, Novoye znaniye, 2013.

11. Kosinova I. I. Ierarhicheskaya Struktura Ehkologicheskogo Monitoringa [The hierarchical structure of ecological and geological monitoring], Monitoring geologicheskih, litologicheskih i ehkologo-geologicheskih sistem [*Monitoring geologistsical, litotehnicheskih and ecological and geological systems*], Moscow, Moscow State Univ., 2007, pp. 24-25.

12. http://www.emercit.ru (accessed 20.09.2016).

13. Kharisova V. N. Global'naya Sputnikovaya radionavigatsionnaya sistema GLONASS [Global Satellite Radionavigation System GLONASS], Moscow, IPRZHR, 2011.

14. http://mssglonass.ru (accessed 30.09.2016).

15. http://www.rfidjournal.com/articles/view?4986 (accessed 25.03.2017).

16. http://www.saymon.info (accessed 25.03.2017).

17. Alguliev R., Mahmudov R. Internet veshchej [Internet of Things], *Informacionnoe obshchestvo [Information Society]*, 2013, no. 3, pp. 42-48.

Применение систем автоматизированного проектирования в машиностроении

Бубнов В. П., Султонов Ш. Х.
Петербургский государственный университет путей сообщения Императора Александра I
Санкт-Петербург, Россия
bubnov1950@yandex.ru, sultonovsh@yandex.ru

Аннотация. **Рассматривается технологический процесс автоматизации твердотельного моделирования на этапе проектно-конструкторских работ. Представлены проблемы, возникающие при использовании программных средств технологического проектирования. Предложено решение этих проблем, которое заключается в автоматическом формировании массива конструктивно-технологических признаков и в синтезе технологического процесса информационной системой на стадии рабочего проектирования.**

Ключевые слова: **твердотельное моделирование, алгоритм, метод конечных элементов, инженерный анализ, SolidWorks, проектирование.**

Введение

В настоящее время одно из важнейших направлений вагоностроения – использование компьютерных технологий для решения сложных задач проектирования. Возможности и границы применения компьютерных технологий для автоматизации проектирования определяются уровнем научно-технических знаний в данной отрасли. Чем глубже разработана теория того или иного класса технических систем, тем больше возможностей для автоматизации процесса их проектирования.

Многие специалисты конструкторских отделов промышленных предприятий приобретают опыт построения твердотельных моделей методом проб и ошибок. В этом случае технология построения трёхмерных моделей с помощью двухмерной системы автоматизированного проектирования не оптимальна и в зависимости от уровня компьютерной подготовки конструктора может быть очень трудоемкой [1, 2].

В последние годы интеллектуальная информационная система (ИИС) для решения расчетных и некоторых проектных задач (изготовления чертежей, спецификаций, расчетов и т. д.) уделяет много внимания автоматизации расчетно-конструкторских работ при проектировании узлов и агрегатов, в связи с чем появляются универсальные инженерные программы. Автоматизация проектирования с помощью компьютерных технологий основывается на системном подходе, т. е. на создании и внедрении систем автоматизированного проектирования технических объектов (САПР), благодаря которым решается весь комплекс задач от анализа задания до разработки полного объема конструкторской и технологической документации [3, 4].

Цели внедрения таких программ – повысить качество проектирования, снизить материальные затраты на него, сократить сроки проектирования и освоения новых видов выпускаемой продукции. Явное преимущество автоматизированного проектирования – возможность заменить математическим моделированием дорогостоящее и продолжительное физическое моделирование. Процесс проектирования реализуется в подсистемах в виде последовательности проектных процедур и операций. Процедура состоит из элементарных проектных операций, имеет твердый порядок их выполнения и направлена на достижение локальной цели в процессе проектирования. Тип объекта проектирования показан на рис. 1.

Рассмотрим пример моделирования автосцепки подвижного состава при помощи программы SolidWorks [4, 5]. Для получения достоверных результатов при расчетах необходимо также рассмотреть условия эксплуатации моделируемой детали или узла.

Автосцепное устройство относится к ответственным частям вагона. Оно предназначено для соединения (сцепления) вагонов и локомотивов, удержания их на определенном расстоянии друг от друга, передачи и смягчения действия

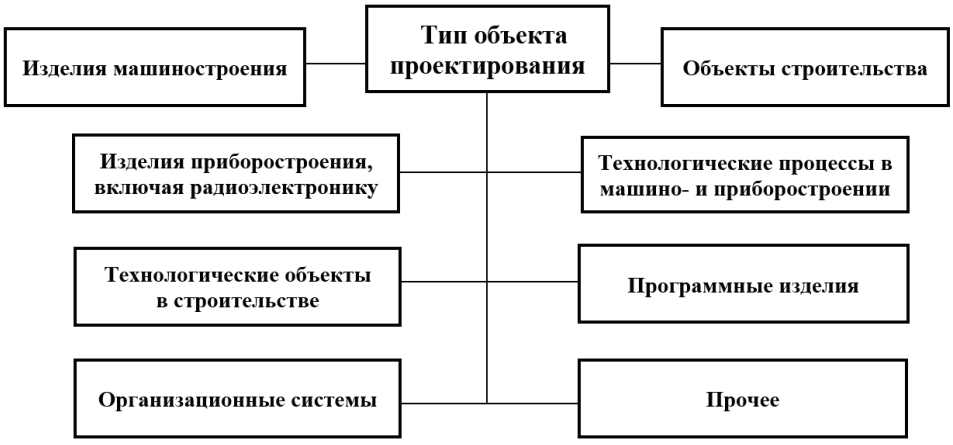


Рис. 1. Тип объекта проектирования

продольных (растягивающих и сжимающих) усилий, развивающихся во время движения поезда.

Нарушения правил эксплуатации (роспуск вагонов с горки на повышенной скорости, неправильное ведение поезда и т. д.) и ремонта автосцепного устройства часто приводят к появлению трещин и изломов в его деталях. Причиной излома может быть и чрезмерный износ деталей.

Автосцепное устройство во время эксплуатации подвергается воздействию комплекса силовых факторов, действующих в вертикальной и горизонтальной плоскостях. Под воздействием перечисленных сил автосцепка одновременно подвергается деформациям изгиба в вертикальной и горизонтальной плоскостях, стесненного кручения, растяжения и сжатия.

С помощью инженерного анализа трехмерного моделирования пользователь может оценить прочность разработанной им конструкции по допустимым напряжениям, определить наиболее слабые места конструкции и внести необходимые изменения в изделие (оптимизировать его). При этом между трехмерной моделью изделия и расчетной конечно-элементной моделью поддерживается ассоциативная связь. Параметрические изменения исходной твердотельной модели автоматически переносятся на сеточную конечно-элементную модель [3]. Алгоритм работы анализ трехмерного моделирование показан на рис. 2.

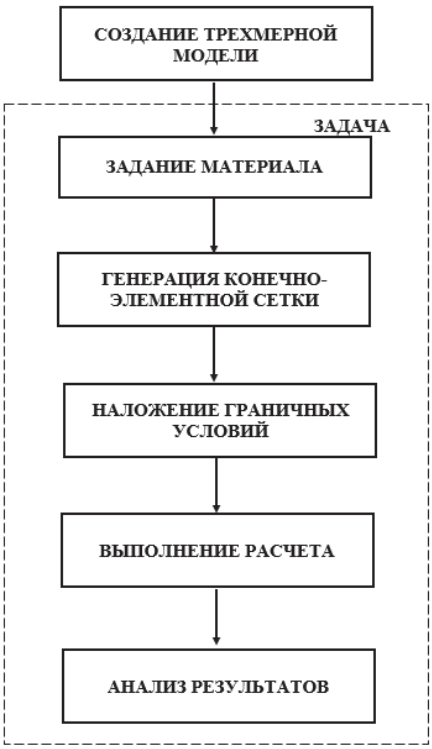


Рис. 2. Алгоритм работы анализа трехмерного моделирования

Смоделируем условия нагружения объекта, чтобы выявить предельную величину значения суммарного продольного зазора в автосцепном устройстве. Для этого необходимо: создать параметризованную модель автосцепки; установить характер взаимодействия объекта с сопряженными элементами (способ опирания); определить типы и места приложения внешних нагрузок; выполнить цикл расчетов; установить тенденцию изменений параметров. Созданная с помощью программы SolidWorks модель автосцепки приведена на рис. 3.

Таким образом, модель есть идеализированное представление заданной реальной конструкции. Точность выполняемого расчета зависит в основном от точности моделирования, поэтому этапу подготовки расчетной модели следует уделять исключительное внимание.

Особенность данного этапа – многовариантность. Для одной и той же конструкции можно создать много моделей. На точность модели влияет степень детальности при отображении реальной конструкции. Иными словами, в модель могут быть включены не все конструктивные элементы, а только те, которые в наибольшей степени определяют ее жесткость и прочность.

Точность моделирования зависит также от размеров используемых конечных элементов и их типов. Основным источником информации служат чертежи. С целью увеличения точности в расчётах при моделировании использованы размеры из чертежей автосцепки СА-3.

На этапе рабочего проектирования, когда имеется окончательный вариант с детальной проработкой, создается подробная расчетная модель, наиболее полно отражающая структуру реальной конструкции.

При генерации сетки конечно-элементной идеализации объекта исследования использовались объёмные конечные элементы. Идеализация автосцепного устройства по МКЭ приведена на рис. 4 [3, 4].

В основе любого расчета на прочность лежит расчетная схема, включающая в себя геометрические параметры конструкций и действующие на нее нагрузки. В дальнейшем в зависимости от конечных целей расчета с учетом материала конструкции определяются напряжения и деформации ее элементов. Затем на основе анализа поля напряжений устанавливается наиболее опасное сечение, при этом

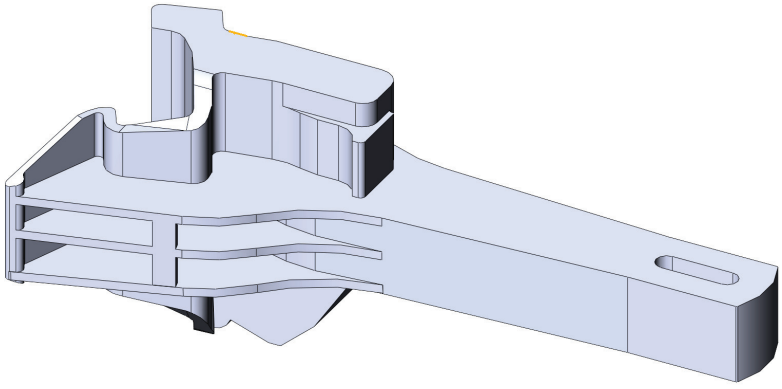


Рис. 3. Конечно-элементная модель автосцепного устройства

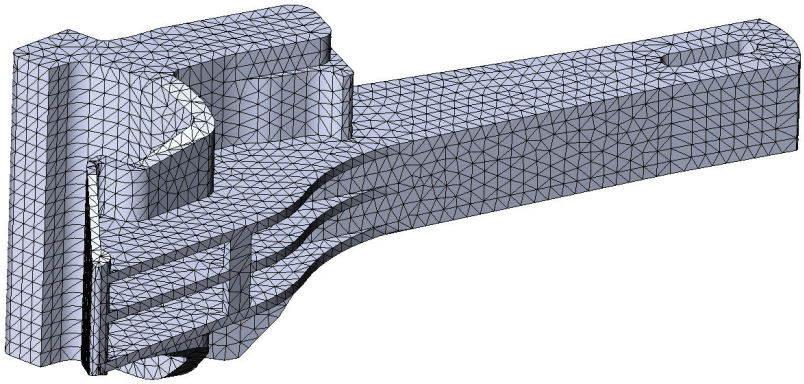


Рис. 4. Подготовка конечно-элементной сетки

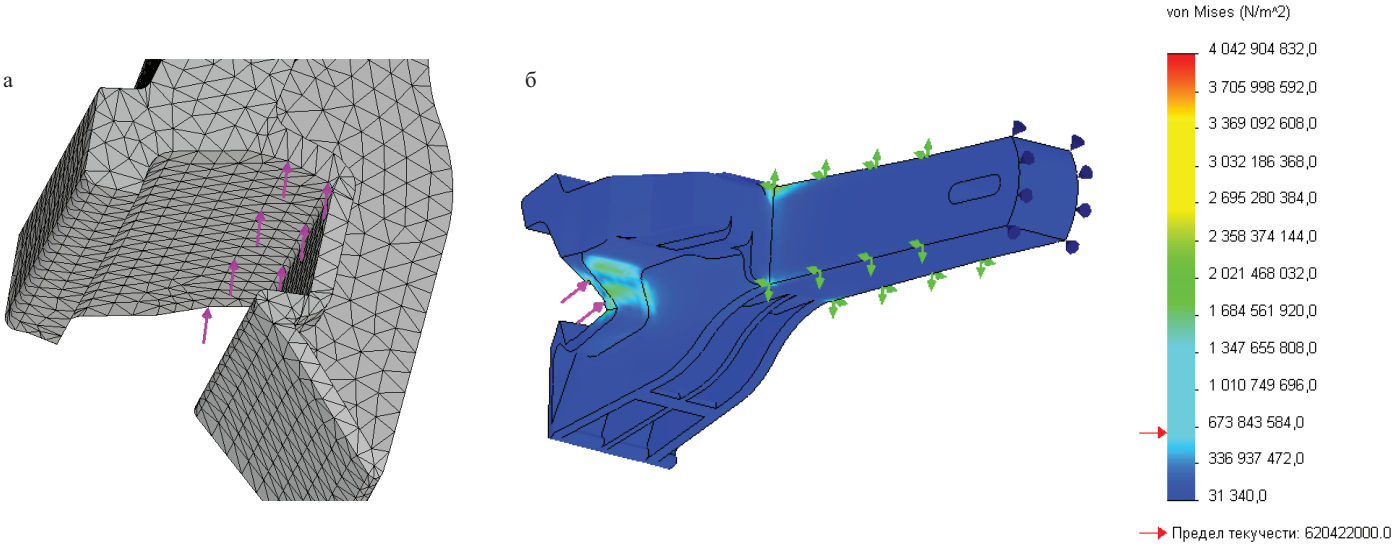


Рис. 5. Установка местоположения внешних нагрузок (а) и моделирование режима толкания (б)

используются гипотезы прочности в зависимости от свойств материала и условий работы конструкции.

В соответствии с конструкторской документацией, марка стали элементов корпуса автосцепки должна быть 20 ГЛ ГОСТ 5267.0-90, допустимое напряжение 295 МПа [6].

При расчетах необходимо правильно установить местоположение и значение внешних нагрузок, вид опирания модели. Моделирование и расчеты производятся для режимов как толкания, так и буксировки. Способ приложения нагрузок и вариант расчета приведен на рис. 5.

Заключение

Моделирование режимов нагружения позволяет установить наиболее нагруженные участки конструкции и места контакта элементов (приложения нагрузок) [6–8].

Литература

1. Radhakrishnan P. CAD/CAM/CIM / P. Radhakrishnan, S. Subramanyan, V. Raju. – New Delhi: New age international publishers, 2004. – 674 p.

2. Hoffmann C. Integrating modeling, simulation, and visualization / C. Hoffmann, V. Popescu, S. Kilic // Computers in Science & Engineering. – 2004. – Vol. 6, no. 1. – P. 52–60.

3. Kurowski P. M. Engineering. Analysis with COSMOS-Works Professional / M. P. Kurowski. – Schroff Development Corporation (SDC), 2005. –248 p.

4. Алямовский А. А. Инженерный анализ методом конечных элементов / А. А. Алямовский. – М.: Проектирование, 2004. – 432 с.

5. Akin J. E. Finite Element Analysis Concepts. Via SolidWorks / J. E. Akin. – New Jersey: World Scientific, 2010. – 335 p.

9. Нормы для расчета и проектирования новых и модернизированных вагонов железных дорог МПС колеи 1520 мм (несамоходных). – М.: ГосНИИВ-ВНИИЖТ, 1996. – 319 с.

7. Fang H. Design and Movement Simulation to the Cam of the Testing Device for capacitor encapsulation equipment / H. Fang, G. Zhang, J. Jian // Open J. Model. Simulation. – 2014. – Vol. 2. – P. 138–143.

8. Кузьмин А. Б. Исследование прочности деталей автосцепки при эксплуатационных нагрузках / А. Б. Кузьмин, В. С. Коссов, А. Л. Протопопов, Н. Ф. Красюков, Б. Б. Бунин, Э. С. Оганьян // Наука и прогресс транспорта. Вестн. Днепропетров. нац. ун-та ж.-д. транспорта. – 2007. – № 19. – С. 170–175.

Application of Computer-Aided Design Systems in Engineering

Bubnov V. P., Sultonov Sh.Kh.
Emperor Alexander I St. Petersburg State Transport University
St. Petersburg, Russia
bubnov1950@yandex.ru, sultonovsh@yandex.ru

Abstract. **The technological process of automation of solid-state modeling at the stage of design and construction work is considered. The problems arising due to the use of software for technological design are presented. The solution of problems by the automatic formation of an array of constructive technological features, and the synthesis of the technological process at the stage of working design by the information system, are proposed.**

Keywords: **solid modeling, algorithm, finite element method, engineering analysis, SolidWorks, design.**

References

1. Radhakrishnan P., Subramanyan S., Raju V. CAD/CAM/CIM, New Delhi, New age international publishers, 2004, 674 p.

2. Hoffmann C., Popescu V., Kilic S. Integrating modeling, simulation, and visualization, *Comput. Sci. & Eng.*, 2004, Vol. 6, no. 1, pp. 52-60.

3. Kurowski P. M. Engineering. Analysis with COSMOS-Works Professional, Schroff Development Corporation (SDC), 2005, 248 p.

4. Alyamovsky A.A. Engineering analysis by the finite element method, Moscow, Designing, 2004, 432 p.

5. Akin J, E. Finite Element Analysis Concepts. Via SolidWorks, New Jersey, World Scientific, 2010, 335 p.

6. Norms for the calculation and design of new and modernized railways of the Ministry of Railways of gauge 1520 mm (non-self-propelled), Moscow, GosNIIV–VNIIZhT, 1996, 319 p.

7. Fang H., Zhang G., Jian J. Design and Movement Simulation to the Cam of the Testing Device for capacitor encapsulation equipment, Open J. Model. and Simulation, 2014, Vol. 2, pp. 138-143.

8. Kuzmin A.B., Kossov A.L., Protopopov N.F., Krasyukov B.B., Bunin E.S. Oganyan Investigation of the strength of the auto-coupling parts under operational loads, *Sci. Transp. Progress. A messenger of the Dnepropetrovsk National Univ. Railway Transp.*, 2007, pp. 170-175.

Опыт реализации дистанционных образовательных технологий при обучении студентов по направлению подготовки «Технология транспортных процессов»

Власенко А. В., Коновалова Т. В., Надирян С. Л.
Кубанский государственный технологический университет
Краснодар, Россия
alex_vlasenko@list.ru

Аннотация. **Рассматривается опыт реализации дистанционных образовательных технологий при обучении студентов по направлению подготовки «Технология транспортных процессов». Описан разработанный авторами алгоритм реализации электронного обучения и дистанционных образовательных технологий. Социологические исследования выявили заинтересованность студентов в применении электронного обучения и дистанционных образовательных технологий при реализации учебного процесса.**

Ключевые слова: образование, обучение, электронное обучение, дистанционные образовательные технологии, электронный программно-методический комплекс.

Обеспечение высокого качества профессиональной подготовки выпускника во многом зависит от выбора образовательных технологий. Образовательный процесс должен обеспечивать активное участие в нем студентов, что позволяет более эффективно и быстро формировать у них компетенции, необходимые для выпускника. Компетентностный подход к обучению позволяет применять практико-ориентированные технологии, при которых студенты погружаются в профессиональную среду во время учебной, технологической, производственной и преддипломной практики.

При проектировании образовательных программ бакалавриата и магистратуры направления подготовки «Технология транспортных процессов» были учтены такие принципы проблемно-ориентированного обучения, как небольшое количество лекций, интегрирующих ряд тем, касающихся решаемых задач и погружающих студентов в проблемный контекст; увеличение объема самостоятельной работы студентов, ориентирование студентов на самостоятельный поиск информации и новых знаний; возможность оценки степени сформированности компетенций [1].

Реализация этих принципов требует изменения функций преподавателя, который должен выступать в роли наставника, консультанта. Для повышения уровня мотивации и вовлеченности студентов в образовательный процесс пересмотрены программы стажировки преподавателей, к учебному процессу привлекаются ведущие специалисты производства (от 5 до 20 %), в рамках учебных курсов систематически проводятся встречи с работодателями, семинары, мастер-классы [2].

Реализуются также современные технологии обучения:

- проблемное обучение;
- проектное обучение;
- инфокоммуникационные технологии;
- технологии сквозного курсового и дипломного проектирования;
- игровое обучение (деловые игры, живое моделирование изучаемых процессов);
- интерактивное обучение.

При изучении инженерных дисциплин наиболее продуктивно используются следующие формы: работа в малых группах, эвристическая беседа, круглый стол (дискуссия, дебаты), мозговой штурм, case-study (кейс-метод, анализ конкретных ситуаций, ситуационный анализ), публичная презентация проекта, дерево решений, мастер-класс [3].

Сочетание базовой фундаментальной подготовки с практико-ориентированной научно-исследовательской работой студентов является основой инновационной системы подготовки выпускников, обладающих не только необходимым объемом знаний, но и навыками самостоятельного решения новых научно-технических задач, подготовленных к работе над проектом в команде, способных за короткое время перестроиться на работу в смежной области знаний и техники [4]. Исследовательская работа студентов в рамках хозяйственных договоров с производственными предприятиями и научно-исследовательскими организациями носит характер междисциплинарного сквозного проектирования [5].

С 2015 г. при обучении студентов бакалавриата и магистратуры по направлению подготовки «Технология транспортных процессов» по всем дисциплинам учебных планов разработаны и внедрены в учебный процесс электронные программно-методические комплексы (ЭПМК). ЭПМК – это электронная копия печатной версии программно-методического комплекса дисциплины, структурированная в виде текстовых и графических файлов, дополненная мультимедийными аудио-, видеофайлами и электронными образовательными ресурсами, предназначенная для реализации дисциплины или ее части с применением электронного обучения и дистанционных образовательных технологий (ЭО и ДОТ).

ЭПМК дисциплин и их функциональные компоненты используются для поддержки учебного процесса с применением ЭО и ДОТ по всем уровням высшего образования и формам обучения в следующих вариантах:

1) применение ЭО и ДОТ в качестве дополнения к традиционной организации учебного процесса путем предостав-

ления студентам возможности самостоятельно изучать учебный материал в рамках реализуемой образовательной программы (просмотр учебно-методических материалов ПМК);

2) применение ЭО и ДОТ с изменением традиционной организации учебного процесса при реализации отдельных видов учебной работы по дисциплине путем сокращения количества аудиторных занятий по дисциплине (лекций, лабораторных, практических занятий и пр.) за счет переноса части занятий в ЭИОС;

3) применение ЭО и ДОТ с изменением традиционной организации учебного процесса при реализации всех видов учебных занятий в рамках отдельной дисциплины ООП путем переноса этих занятий в ЭИОС (кроме проведения промежуточной аттестации) [6].

Требования к структуре, содержанию, оформлению, разработке, утверждению, регистрации и пересмотру ЭПМК дисциплины и его компонентов, используемых при реализации основных образовательных программ с применением ЭО и ДОТ, определены стандартом образовательной организации.

ЭПМК 28 % дисциплин учебных планов бакалавриата и магистратуры направления подготовки «Технология транспортных процессов» и их функциональные компоненты разработаны для 3-го варианта применения: предполагают обратную связь студентов с преподавателем (on- и offline мероприятия: вебинары, переписку, тестирование, индивидуальные и групповые консультации и пр.). Электронное обучение реализуется без освобождения студентов от посещения аудиторных занятий.

В ЭПМК размещены в формате .pdf рабочая программа дисциплины, конспект лекций, список литературы, типовые контрольные задания, вопросы к экзамену, методические указания к практическим занятиям, по выполнению курсовой работы, по изучению дисциплины, по самостоятельной работе. Глоссарий по дисциплине содержит около 100 терминов, что способствует усвоению студентами лекционного материала при изучении курса.

В интерактивном режиме студентам доступны:

• конспект лекций. Форма предоставления материала позволяет студентам обращаться к глоссарию по дисциплине, источникам литературы, нормативным документам, а также возвращаться к другим разделам курса, что дает возможность усваивать материал каждой лекции и понимать место изучаемого вопроса в дисциплине в целом;

• консультации преподавателя. В рамках разработанного ЭПМК у студентов имеется возможность задать вопросы преподавателю, отправить работу на проверку. Данная форма получения консультации позволяет во время аудиторных занятий уделять больше времени разъяснению проблемных вопросов по теме практических работ, повышает степень самостоятельности выполняемых заданий, способствует более глубокому пониманию изучаемой дисциплины. В результате такого взаимодействия преподавателя и студентов наблюдается большая степень оригинальности проектных решений;

• тесты. В ЭПМК предусмотрены три уровня проверки знаний студентов: тестовые задания для перехода от одной части лекции к другой, тесты по каждому разделу дисциплины и итоговый тест по курсу. Данная форма проверки знаний повышает уровень подготовленности студентов к каждому занятию и к промежуточной аттестации. В перспективе возникает возможность вводить рейтинговую оценку знаний студентов, вносить преподавателю коррективы в изложение материалов лекций и практических занятий (в методическом плане).

При реализации электронного обучения оперативно решаются вопросы организационного характера: время и место консультаций, особенности оформления курсовой работы и отчетов по практическим занятиям и т. п.

При апробации модели электронного обучения по направлению подготовки «Технология транспортных процессов» (бакалавриат и магистратура) выявлены следующие проблемы: необходимо дополнительное обучение студентов работе в информационной образовательной среде; наблюдается низкая активность студентов в межсессионный период; преподаватель затрачивает дополнительное время на работу со студентами.

Литература

1. Заровная Л. С. Особенности преподавания дисциплины «Основы научных исследований и защита интеллектуальной собственности» для направления подготовки «Технология транспортных процессов» / Л. С. Заровная, Т. В. Коновалова, Н. В. Магзумова // Технологии транспортных процессов на Дону – 2016. – Новочеркасск, 2016. – С. 141–144.

2. Коновалова Т. В. Исследование результатов реализации электронного обучения и дистанционных образовательных технологий в ФГБОУ ВО «КубГТУ» / Т. В. Коновалова, Л. М. Малука, С. А. Арефьева, С. Л. Надирян // Гуманитарные, социально-экономические и общественные науки. – 2016. – № 10. – С. 73–75.

3. Москвич В. К. Опыт проектирования и реализации основных образовательных программ магистратуры / В. К. Москвич, Т. В. Коновалова // Прогрессивные технологии в транспортных системах. – Оренбург, 2013. – С. 367–370.

4. Modern information and communication technologies in higher education: new education programs, pedagogic with the use of e-learning and education improvement. The I international workshop conference. – Moscow; Sapienza Univ. Rome, National Res. Univ. Electronic Technology (MIET), Bauman Moscow State Tech. Univ., Inst. Qualification Improvement and Vocational Retraining, 2013.

5. Tadevosyan A. B. Application of information technologies of «electronic education» in higher education as a necessary condition of overcoming the modern crisis and successful development in xxi-st century / A. B. Tadevosyan // Бизнес-информ. – 2012. – № 7. – С. 245–247.

6. Raevneva E. V. Theoretical and methodological grounds of formation of the efficient system of higher education / E. V. Raevneva, I. V. Aksionova, M. F. Goncharenko // Problems of Economics. – 2013. – № 3. – С. 28–33.

Experience of implementation of distance educational technologies in training of students in specialty “Technology of transport processes”

Vlasenko A. V., Konovalova T. V., Nadiryan S. L.
Kuban state technological University
Krasnodar, Russia
alex_vlasenko@list.ru

Abstract. This article examines the experience of implementation of distance educational technologies in training of students in specialty “Technology of transport processes”. Describes the authors developed the algorithm of implementation of e-learning and distance educational technologies. Sociological research has identified students ‘ interest in further implementation of the educational process with the use of e-learning and distance educational technologies.

Keywords: education, training, discipline, e-learning, distance educational technologies, the electronic program and methodical complex.

References

1. Zarowna L. S., Konovalova T. V., Magzumova N. V. Osobennosti prepodavaniya discipliny “Osnovy nauchnyh issledovanij i zashchita intellektual’noj sobstvennosti” dlya napravleniya podgotovki “Tekhnologiya transportnyh processov” [Features of teaching of discipline “Bases of scientific researches and protection of intellectual property” for the specialty “Technology of transport processes”], Tekhnologii transportnyh processov na Donu – 2016 *[Technology of transport processes-on-Don in 2016]*, Novocherkassk, 2016, pp. 141–144.

2. Konovalova T. V., Maluca L. M., Aref’eva S. A. Issledovanie rezul’tatov realizacii ehlektronnogo obucheniya i distancionnyh obrazovatel’nyh tekhnologij v FGBOU VO “KubGTU” [Nadiryan S. L. A study of the results of the implementation of e-learning and distance educational technologies of the “Kuban state University”], Gumanitarnye, social’no-ehkonomicheskie i obshchestvennye nauki [*Humanitarian, Socio-Econ. Soc. Sci.*], 2016, no. 10, pp. 73-75.

3. Moskvich V. K., Konovalova T. V. Opyt proektirovaniya i realizacii osnovnyh obrazovatel’nyh programm magistratury [Experience in the design and implementation of basic educational programs of magistracy], *Progressivnye tekhnologii v transportnyh sistemah [Progressive technologies in transport systems]*, Orenburg, 2013, pp. 367-370.

4. Modern information and communication technologies in higher education: new education programs, with the pedagogic use of e-learning and education improvement. The I international conference workshop. Moscow, Sapienza Univ. Rome, National Res. Univ. Electronic Technology (MIET), Bauman Moscow State Tech. Univ., Inst. Qualification Improvement and Vocational Retraining, 2013.

5. Tadevosyan A. B. Application of information technologies of “electronic education” in higher education as a necessary condition of overcoming the modern crisis and successful development in the XXI-st century, *Business inform*, 2012, no. 7, pp. 245-247.

6. Raevneva E. V., Aksionova I. V., Goncharenko M. F. Theoretical and methodological grounds of formation of the efficient system of higher education, *Problems of Economics*, 2013, no. 3, pp. 28-33.

Список авторов статей, опубликованных в № 1 журнала «Интеллектуальные технологии на транспорте» за 2017 год

Александрова Елена Борисовна
д. т. н., доцент
Должность: профессор кафедры «Информационная безопасность компьютерных систем» ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого».
Область научных интересов: информационная безопасность, криптография, алгебраическая геометрия.
E-mail: helen@ibks.spbstu.ru

Бубнов Владимир Петрович
д. т. н., профессор
Должность: профессор кафедры «Информационные и вычислительные системы» ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I».
Область научных интересов: моделирование сложных систем, системы массового обслуживания, надежность программного обеспечения.
E-mail: bubnov1950@yandex.ru

Власенко Александра Владимировна
к. т. н., доцент
Должность: доцент кафедры компьютерных технологий и информационной безопасности института информационных технологий и безопасности, начальник управления аспирантуры и докторантуры ФГБОУ ВО «Кубанский государственный технологический университет».
Область научных интересов: экономика защиты информации, экономические аспекты безопасности компьютерных систем и автоматизированных систем.
E-mail: alex_vlasenko@list.ru

Зегжда Дмитрий Петрович
д. т. н., профессор
Должность: заведующий кафедрой «Информационная безопасность компьютерных систем» ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого».
Область научных интересов: информационная безопасность, облачные вычисления, виртуализация, теория графов, анализ безопасности.
E-mail: dmitry.zegzhda@ibks.ftk.spbstu.ru

Коновалова Татьяна Вячеславовна
к. э. н., доцент
Должность: заведующий, доцент кафедры Организации перевозок и дорожного движения ФГБОУ ВО «Кубанский государственный технологический университет».
Область научных интересов: логистика, транспорт, оценка эффективности организации дорожного движения, транспортная инфраструктура.
E-mail: tan_kon@mail.ru

Лаврова Дарья Сергеевна
к. т. н.
Должность: ассистент кафедры «Информационная безопасность компьютерных систем» ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого».
Область научных интересов: информационная безопасность, обнаружение инцидентов безопасности, SIEM.
E-mail: lavrova@ibks.spbstu.ru

Надирян София Левоновна
Должность: ассистент кафедры «Организации перевозок и дорожного движения» ФГБОУ ВО «Кубанский государственный технологический университет».
Область научных интересов: вычислительная техника и сети на транспорте, системы автоматизации на автомобильном транспорте, логистика.
E-mail: sofi008008@yandex.ru

Носкова Александра Игоревна
магистр ФГБОУ ВО «Петербургский университет путей сообщения Императора Александра I».
Область научных интересов: информационные системы, базы данных.
E-mail: alexandranskv@mail.ru

Смагин Владимир Александрович
д. т. н., профессор, ЗДНРФ
Должность: профессор кафедры метрологического обеспечения Военно-космической академии им. А. Ф. Можайского.
Область научных интересов: теория надёжности, теория информации, теория случайных процессов и нечётких множеств.
E-mail: va_smagin@mail.ru

Султонов Шохрух Холмурзаевич
магистрант кафедры «Информационные и вычислительные системы» ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I».
Область научных интересов: моделирование сложных систем, надежность программного обеспечения.
E-mail: sultonovsh@yandex.ru

Токранова Мария Вадимовна
магистр ФГБОУ ВО «Петербургский государственный университет путей сообщения императора Александра I».
Область научных интересов: информационные системы, базы данных.
E-mail: mari_tn@mail.ru

Фомичева Светлана Григорьевна
к. т. н., профессор
Должность: заведующая кафедрой «Информационных систем и технологий» ФГБОУ ВО «Норильский государственный индустриальный институт».
Область научных интересов: распределенные информационно-телекоммуникационные системы, информационная безопасность, интеллектуальные системы.
E-mail: Levikha@rambler.ru

Шмелев Валентин Валерьевич
к. т. н.
Должность: докторант Военно-космической академии им. А. Ф. Можайского.
Область научных интересов: автоматизированные системы управления в ракетно-космической отрасли, обработка и анализ телеметрической информации.
E-mail: valja1978@yandex.ru

The list of authors of articles published in the journal number 1 «Intellectual Technologies on Transport» for 2017

Aleksandrova Elena Borisovna
Doct. Eng., docent
Appointment: professor of the Department «Information security of computer systems» Saint Petersburg State Polytechnic University.
Academic interests: information security, cryptography, algebraic geometry.
E-mail: helen@ibks.spbstu.ru

Bubnov Vladimir Petrovich
Doct. Eng.
Appointment: professor of "Information Technology Systems", Emperor Alexander I St. Petersburg State Transport University.
Academic interests: Modeling of complex systems, queuing systems, software reliability.
E-mail: bubnov1950@yandex.ru

Fomicheva Svetlana Grigorievna
Cand. Eng., professor
Appointment: Head of Chair «Information systems & technologies» Norilsk State Industrial Institute.
Academic interests: distributed information-telecommunication systems, information security, intelligent systems.
E-mail: Levikha@rambler.ru

Konovalova Tatyana Vyacheslavovna
Cand. Ekon. Sciences, associate Professor
Appointment: head, associate Professor of transportation and traffic FGBOU „Kuban state technological University".
Academic interests: logistics, transport, assessment of the efficiency of road traffic organization, transport infrastructure.
E-mail: tan_kon@mail.ru

Lavrova Daria Sergeevna
Cand. Eng.
Appointment: professor assistant of the Department «Information security of computer systems» Saint Petersburg State Polytechnic University.
Academic interests: information security, detection of security incidents, SIEM.
E-mail: lavrova@ibks.spbstu.ru

Nadiryan Sofiya Levonovna
Appointment: assistant of the Department "Organization of transportation and road traffic" FGBOU „Kuban state technological University".
Academic interests: computer technology and networks in transport, automation systems for road transport, logistics.
E-mail: sofi008008@yandex.ru

Noskova Aleksandra Igorevna
Master of the Emperor Alexander I Petersburg state transport University.
Academic interests: information systems, databases.
E-mail: alexandranskv@mail.ru

Shmelev Valentin Valerievich
Cand. Eng.
Appointment: doctoral student of the AF Mozhaisky Military Space Academy.
Academic interests: Automated control systems in the rocket and space industry, processing and analysis of telemetric information.
E-mail: valja1978@yandex.ru

Smagin Vladimir Aleksandrovich
Doc. Eng., professor, 3DSRF
Appointment: professor of department of metrological support of Military space academy name A. F. Mozhaisk.
Academic interests: theory of reliability, theory of information, theory of accidental processes and indistinct sets.
E-mail: va_smagin@mail.ru

Sultonov Shokhrukh Kholmurzaevich
Graduate student of "Information Technology Systems", Emperor Alexander I St. Petersburg State Transport University.
Academic interests: Modeling of complex systems, reliability of software.
E-mail: sultonovsh@yandex.ru

Tokranova Maria Vadimovna
Master Emperor Alexander I St. Petersburg State Transport University.
Academic interests: information systems, databases.
E-mail: mari_tn@mail.ru

Vlasenko Alexandra Vladimirovna
Cand. Eng., associate Professor
Appointment: Department of computer technologies and information security Institute of information technology and security, head of Department of postgraduate and doctoral studies in FGBOU "Kuban state technological University".
Academic interests: economics of information protection, economic aspects of security of computer systems and automated systems.
E-mail: alex_vlasenko@list.ru

Zegzhda Dmitry Petrovich
Doc. Eng., professor
Appointment: head of the Department «Information security of computer systems» Saint Petersburg State Polytechnic University.
Academic interests: information security, cloud computing, virtualization, graph theory, security analysis.
E-mail: dmitry.zegzhda@ibks.ftk.spbstu.ru